

UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

TIMOTHY H. EDGAR et al.,

Plaintiffs,

v.

DANIEL COATS, in his official capacity as
Director of National Intelligence, et al.,

Defendants.

Case No. 8:19-cv-00985 (GJH)

DECLARATION OF ALEX ABDO

I, Alex Abdo, a member of the Bar of the State of New York, declare under penalty of perjury as follows. I am the litigation director of the Knight First Amendment Institute at Columbia University, and I represent Plaintiffs in this matter. I submit this declaration in support of Plaintiffs' Memorandum of Law in Opposition to Defendants' Motion to Dismiss. Attached to this declaration are true and correct copies of the following documents¹:

CIA

AR 13-10, *Agency Prepublication Review of
Certain Material Prepared for Public
Dissemination* (June 25, 2011)A

*Keeping Secrets Safe: The Publications Review
Board*, CIA (Nov. 1, 2018),
[https://www.cia.gov/about-cia/publications-review-
board](https://www.cia.gov/about-cia/publications-review-board) [<https://perma.cc/QLU9-X7RK>]B

¹ Exhibits A, H, I, and J were produced by the government to the American Civil Liberties Union and the Knight First Amendment Institute in response to a Freedom of Information Act request.

DOD

DD Form 1847-1, *Sensitive Compartmented Information Nondisclosure Statement* (Dec. 1991),
https://fas.org/sgp/othergov/dd_1847_1.pdf
[<https://perma.cc/Q63X-PJXD>] C

DOD Directive 5230.09, *Clearance of DoD Information for Public Release* (Apr. 14, 2017),
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/523009p.pdf>
[<https://perma.cc/L727-VKR7>] D

DOD Instruction 5230.09, *Clearance of DoD Information for Public Release* (Jan. 25, 2019),
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/523009p.pdf>
[<https://perma.cc/ZYU8-ZFHS>] E

DOD Instruction 5230.29, *Security and Policy Review of DoD Information for Public Release* (Apr. 14, 2017),
<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/523029p.pdf>
[<https://perma.cc/W7BB-HQKG>] F

Frequently Asked Questions for Department of Defense Security and Policy Reviews, DOD (Mar. 2012),
<http://www.dami.army.pentagon.mil/site/InfoSec/docs/Topics/Pre-Publication%20Pamphlet%20FAQ%20March%202012.pdf> [<https://perma.cc/5AH3-S3RV>] G

NSA

NSA/CSS Policy 1-30, *Review of NSA/CSS Information Intended for Public Release* (May 12, 2017) H

ODNI

Form 313, *Nondisclosure Agreement for Classified Information* (Dec. 2016) I

Instruction 80.04, Revision 2, *ODNI Pre-Publication Review of Information to Be Publicly Released* (Aug. 9, 2016) J

Shared non-disclosure agreements

Standard Form 312, *Classified Information
Nondisclosure Agreement* (July 2013),
<https://fas.org/sgp/othergov/sf312.pdf>
[<https://perma.cc/29QD-3ZZB>]K

Form 4414, *Sensitive Compartmented Information
Nondisclosure Agreement* (Dec. 2013),
<https://fas.org/sgp/othergov/intel/sf4414.pdf>
[<https://perma.cc/28RJ-N364>] L

Dated: July 16, 2019

Respectfully submitted,

Brett Max Kaufman*
Vera Eidelman*
Naomi Gilens*
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
T: 212.549.2500
F: 212.549.2654
bkaufman@aclu.org
veidelman@aclu.org
ngilens@aclu.org

/s/ Alex Abdo
Alex Abdo*
Jameel Jaffer*
Ramya Krishnan*
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
T: 646.745.8500
alex.abdo@knightcolumbia.org
jameel.jaffer@knightcolumbia.org
ramya.krishnan@knightcolumbia.org

David R. Rocah (Bar No. 27315)
American Civil Liberties Union Foundation
of Maryland
3600 Clipper Mill Road, Suite 350
Baltimore, MD 21211
T: 410.889.8555
F: 410.366.7838
rocah@aclu-md.org

* admitted *pro hac vice*

Counsel for Plaintiffs

EXHIBIT A:

AR 13-10, *Agency*
Prepublication Review of
Certain Material Prepared for
Public Dissemination
(June 25, 2011)

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
Approved for Release: 2017/04/06 C06652547

UNCLASSIFIED//~~FOUO~~

(U) Disseminating or sharing any part of this document outside CIA must comply with AR 10-16.

AR 13-10 (U//~~FOUO~~) AGENCY PREPUBLICATION REVIEW OF CERTAIN MATERIAL PREPARED FOR PUBLIC DISSEMINATION (Formerly AR 6-2)

AGENCY REGULATION SERIES 13 (SPECIAL REPORTING REQUIREMENTS/RESTRICTIONS), PUBLISHED ON 25 JUNE 2011

Regulation Summary

Ingested from Regulations.cia on 10 May 2013

Policy

REVISION SUMMARY: 25 June 2011

This regulation supersedes AR 6-2, dated 19 July 2010.

AR 6-2 is revised to clarify the prepublishation review criteria applicable to the submissions of current CIA employees and contractors and to reflect current organizational titles, existing Board membership, and updated citations to certain applicable authorities.

Boldfaced text in this regulation indicates revisions.

(b)(3) CIAAct

This regulation was written by the Office of the Chief Information Officer,

2. (U//~~FOUO~~) AGENCY PREPUBLICATION REVIEW OF CERTAIN MATERIAL PREPARED FOR PUBLIC DISSEMINATION

(U//~~FOUO~~) SYNOPSIS. This regulation sets forth CIA policies and procedures for the submission and review of material proposed for publication or public dissemination by current and former employees and contractors and other individuals obligated by the CIA secrecy agreement to protect from unauthorized disclosure certain information they obtain as a result of their contact with the CIA. This regulation applies to all forms of dissemination, whether in written, oral, electronic, or other forms, and whether intended to be an official or nonofficial (that is, personal) publication.

- a. **(U//~~FOUO~~) AUTHORITY.** The National Security Act of 1947, as amended, the Central Intelligence Agency (CIA) Act of 1949, as amended, and Executive Order 12333, **as amended**, require the protection of intelligence sources and methods from unauthorized disclosure. Executive Order 13526, requires protection of classified information from unauthorized disclosure. 18 U.S.C. section 209 prohibits a federal employee from supplementation of salary from any source other than the U.S. Government as compensation for activities related to the employee's service as a Government employee. The *Standards of Ethical Conduct for Employees of the Executive Branch* (5 C.F.R. 2635) are the Government-wide ethics regulations that govern Federal employees. Those regulations include restrictions on outside activities and compensation for teaching, speaking, and writing related to official duties. In *Snepp v. U.S.*, 444 U.S. 507 (1980), the Supreme Court held that individuals who have been authorized access to CIA information, the public disclosure of which could harm the national security, hold positions of special trust and have fiduciary obligations to protect such information. These obligations are reflected in this regulation and in CIA secrecy agreements.

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
Approved for Release: 2017/04/06 C06652547

UNCLASSIFIED//~~FOUO~~

b. (U//~~FOUO~~) GENERAL REQUIREMENTS AND DEFINITIONS

- (1) The CIA requires all current and former Agency employees and contractors, and others who are obligated by CIA secrecy agreement, to submit for prepublication review to the CIA's Publications Review Board (PRB) all intelligence-related materials intended for publication or public dissemination, whether they will be communicated in writing, speeches, or any other method; and whether they are officially sanctioned or represent personal expressions, except as noted below.
- (2) The purpose of prepublication review is to ensure that information damaging to the national security is not disclosed inadvertently; and, for current employees and contractors, to ensure that neither the author's performance of duties, the Agency's mission, nor the foreign relations or security of the U.S. are adversely affected by publication.
- (3) The prepublication review requirement does not apply to material that is unrelated to intelligence, foreign relations, or CIA employment or contract matters (for example, material that relates to cooking, stamp collecting, sports, fraternal organizations, and so forth).
- (4) Agency approval for publication of nonofficial, personal works (including those of current and former employees and contractors and covered non-Agency personnel) does not represent Agency endorsement or verification of, or agreement with, such works. Therefore, consistent with cover status, authors are required, unless waived in writing by the PRB, to publish the following disclaimer:

"All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the Central Intelligence Agency (CIA) or any other U.S. Government agency. Nothing in the contents should be construed as asserting or implying U.S. Government authentication of information or CIA endorsement of the author's views. This material has been reviewed by the CIA to prevent the disclosure of classified information."

- (5) Those who are speaking in a nonofficial capacity must state at the beginning of their remarks or interview that their views do not necessarily reflect the official views of the CIA.
- (6) A nonofficial or personal publication is a work by anyone who has signed a CIA secrecy agreement (including a current and former employee or contractor), who has prepared the work as a private individual and who is not acting in an official capacity for the Government.
- (7) An official publication is a work by anyone who has signed a CIA secrecy agreement, (including a current employee or contractor), such as an article, monograph, or speech, that is intended to be unclassified and is prepared as part of their official duties as a Government employee or contractor acting in an official capacity.
- (8) "Publication" or "public dissemination" in this context means:
 - (a) for nonofficial (that is, personal) works -- communicating information to one or more persons; and
 - (b) for official works -- communicating information in an unclassified manner where that information is intended, or is likely to be, disseminated to the public or the media.
- (9) Covered non-Agency personnel means individuals who are obligated by a CIA secrecy agreement to protect from unauthorized disclosure certain information they obtain as a result of

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
Approved for Release: 2017/04/06 C06652547

UNCLASSIFIED//~~AWG~~

their contact with the CIA.

c. (U//~~AWG~~) THE PUBLICATIONS REVIEW BOARD

- (1) The PRB is the Agency body charged with reviewing, coordinating, and formally approving in writing all proposed nonofficial, personal publications that are submitted for prepublication. It is also responsible for coordinating the official release of certain unclassified Agency information to the public. The Board consists of a Chair and senior representatives from the Director of CIA Area, the National Clandestine Service (NCS), the Directorate of Support, the Directorate of Science and Technology, and the Directorate of Intelligence. **There is a nonvoting Executive Secretary** and the Office of General Counsel (OGC) provides a nonvoting legal advisor.
- (2) The PRB shall adopt and implement all lawful measures to prevent the publication of information that could damage the national security or foreign relations of the U.S. or adversely affect the CIA's functions or the author's performance of duties, and to ensure that individuals given access to classified information understand and comply with their contractual obligations not to disclose it. When the PRB reviews submissions that involve the equities of any other agency, the PRB shall coordinate its review with the equity-owning agency.
- (3) The PRB Chair is authorized unilaterally to represent the Board when disclosure of submitted material so clearly would not harm national security that additional review is unnecessary or when time constraints or other unusual circumstances make it impractical or impossible to convene or consult with the Board. The Chair may also determine that the subject of the material is so narrow or technical that only certain Board members need to be consulted.
- (4) During the course of PRB deliberations, the views of the equity-owning Board member regarding damage to national security and appropriateness for publication will be given great weight. In the even the PRB Chair and other Board members disagree as to whether the publication of information could damage the national security or if the *Studies in Intelligence* Editorial Board Chair disagrees with a PRB decision under section g(2) below that an article is inappropriate for publication, the PRB Chair, or Director of the Center for the Study of Intelligence, will have 15 days to raise the issue to the Chief, IMS for review, highlighting the equity-owner's concerns. If no resolution is reached at that level, the C/IMS will have 15 days to raise the matter to the Associate Deputy Director of the Central Intelligence Agency (ADD/CIA) for a final decision. When there is a disagreement whether information should be approved for publication, it will not be so approved until the issue is resolved by the C/IMS or the ADD/CIA. However, if the issue is not raised to the C/IMS or the ADD/CIA within the applicable time limits, the views of the equity-owning Board member will be adopted as the decision of the PRB (or in those cases where the *Studies of Intelligence* Editorial Board Chair disagrees with the PRB decision and the issue is not raised within applicable time limits, the PRB decision will be final).

d. (U//~~AWG~~) CONTACTING THE PRB

- (1) Former employees and contractors and other covered non-Agency personnel must submit covered nonofficial (personal) materials intended for publication or public dissemination to the PRB by mail, fax, or electronically as follows:

For U.S. Mail:

CIA Publications Review Board



(b)(3) CIAAct

AR 13-10

UNCLASSIFIED//~~AWG~~

3 of 9

000012
Approved for Release: 2017/04/06 C06652547

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
Approved for Release: 2017/04/06 C06652547

UNCLASSIFIED//AIUO

Washington, DC 20505

For Overnight Delivery (for example, FedEx, UPS, and so forth):

[Redacted box]

(b)(3) CIAAct

Facsimile: [Redacted box]

(b)(3) CIAAct

Email: [Redacted box]

(b)(3) CIAAct

Phone: [Redacted box]

(b)(3) CIAAct

- (2) Current employees and contractors must submit covered nonofficial and official materials intended for publication or public dissemination to the PRB by mail, fax, or electronically as follows:

Internal Mail: [Redacted box]

(b)(3) CIAAct

Classified Facsimile: [Redacted box]

(b)(3) CIAAct

Email: Lotus Note to: [Redacted box]

(b)(3) CIAAct

Secure Phone: [Redacted box]

(b)(3) CIAAct

- (3) Current employees and contractors intending to publish or speak on a nonofficial personal basis must also complete and submit to the PRB an electronic cover memorandum identifying their immediate supervisor or contracting officer. The PRB will notify the appropriate Agency manager or contracting officer, whose concurrence is necessary for publication.

- (4) Review Timelines. As a general rule, the PRB will complete prepublication review for nonofficial publications within 30 days of receipt of the material. Relatively short, time-sensitive submissions (for example, op-ed pieces, letters to the editor, and so forth) will be handled as expeditiously as practicable. Lengthy or complex submissions may require a longer period of time for review, especially if they involve intelligence sources and methods issues. Authors are strongly encouraged to submit drafts of completed works, rather than chapters or portions of such works.

e. (U//~~AIUO~~) WHAT IS COVERED

- (1) Types of Materials. The prepublication review obligation applies to any written, oral, electronic, or other presentation intended for publication or public dissemination, whether personal or official, that mentions CIA or intelligence data or activities or material on any subject about which the author has had access to classified information in the course of his employment or other contact with the Agency. The obligation includes, but is not limited to, works of fiction; books; newspaper columns; academic journal articles; magazine articles; resumes or biographical information on Agency employees (submission to the PRB is the exclusive

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
 Approved for Release: 2017/04/06 C06652547

UNCLASSIFIED//~~FOUO~~

procedure for obtaining approval of proposed resume text); draft *Studies in Intelligence* submissions (whenever the author is informed by the *Studies* editor that the draft article is suitable for *Studies* Editorial Board review); letters to the editor; book reviews; pamphlets; scholarly papers; scripts; screenplays; internet blogs, e-mails, or other writings; outlines of oral presentations; speeches; or testimony prepared for a Federal or state or local executive, legislative, judicial, or administrative entity; and Officers in Residence (OIRs) speeches and publications (although oral and written materials prepared by OIRs exclusively for their classroom instructional purposes are not covered, OIRs must take particular care to ensure that any anecdotes or other classroom discussions of their Agency experiences do not inadvertently reveal classified information). Materials created for submission to the Inspector General and/or the Congress under the Whistleblower Protection Act and CIA implementing regulations are nonofficial, personal documents when they are initially created and the author is entitled to seek a review by the PRB to determine if the materials contain classified information and, if so, the appropriate level of classification of the information. If, at any point during or after the whistleblower process, the author wishes to disseminate his whistleblower complaint to the public, the author must submit his complaint to the PRB for full prepublication review under this regulation. If the author is a current employee or contractor who intends to disseminate his whistleblower complaint to the public, the author must also obtain PRB review of his materials under paragraph g below.

- (2) Review of Draft Documents. Written materials of a nonofficial, personal nature covered by the regulation must be submitted to the PRB at each stage of their development before being circulated to publishers, editors, literary agents, co-authors, ghost writers, reviewers, or the public (that is, anyone who does not have the requisite clearance and need-to-know to see information that has not yet been reviewed, but may be classified). This prepublication review requirement is intended to prevent comparison of different versions of such material, which would reveal the items that the Agency has deleted. For this reason, PRB review of material only after it has been submitted to publishers, reviewers, or other outside parties violates the author's prepublication review obligation. The Agency reserves the right to conduct a post-publication review of any such material in order to take necessary protective action to mitigate damage caused by such a disclosure. Such post-publication review and action does not preclude the U.S. Government or the CIA from exercising any other legal rights otherwise available as a result of this prepublication violation. Additionally, the Agency reserves the right to require the destruction or return to CIA of classified information found to have been included in earlier versions of a work regardless of the form of the media involved (for example, paper, floppy disk, hard disk, or other electronic storage methods).

(3) Public Presentations.

- (a) With respect to current and former employees and contractors and covered non-Agency personnel making intelligence-related speeches, media interviews, or testimony, they must submit all notes, outlines, or any tangible preparatory material to the PRB for review. Where no written material has been prepared specifically in contemplation of the speech, interview, or oral testimony, the individual must contact the PRB Chair or his representative to provide a summary of any and all topics that it is reasonable to assume may be discussed, and points that will or may be made. Unprepared or unrehearsed oral statements do not exempt an individual from possible criminal liability in the event they involve an unauthorized disclosure of classified information.
- (b) In addition, with respect to current employees and contractors making official or nonofficial oral intelligence-related statements to the media or to groups where the media will likely be

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
Approved for Release: 2017/04/06 C06652547

UNCLASSIFIED//~~FOUO~~

in attendance, prior to granting interviews or making public appearances, the speaker shall contact the PRB for guidance. The PRB will coordinate the review of proposed speeches or media interviews with the component involved, the Office of Public Affairs for guidance regarding media or press relations, and other offices as necessary.

(c) Current employees who must make court appearances or respond to subpoenas must contact OGC for guidance.

(4) Official Publications. The publication or public dissemination of official Agency information by any means, including electronic transmissions, such as internet and unclassified facsimile, is subject to prepublication review. In addition to the types of materials listed in paragraph e(1) above, official publications subject to this review include unclassified monographs; organizational charts; brochures; booklets; flyers; posters; advertisements; films; slides; videotapes; or other issuances, irrespective of physical media such as paper, film, magnetic, optical, or electronic, that mention CIA or intelligence data or activities or material on any subject about which the author has had access to classified information in the course of his employment or other association with the Agency.

(5) Exclusions. Not included within the scope of this regulation are CIA court filings; regular, serial publications such as the *CIA World Fact Book*; or documents released pursuant to official declassification and release programs such as the Freedom of Information Act or the 25-Year Automatic Declassification Program under Executive Order 13526. Nor do these procedures apply to official documents intended to be disseminated only to other Federal Government entities (that is, responses to other Federal agencies and Congressional entities -- except for unclassified "constituent replies" that will remain covered by this regulation).

(6) Additional PRB Guidance. It is not possible to anticipate all questions that may arise about which materials require prepublication review. Therefore, it is the author's obligation to seek guidance from the PRB on all prepublication review issues not explicitly covered by this regulation.

f. (U//~~FOUO~~) PREPUBLICATION REVIEW GUIDELINES FOR FORMER EMPLOYEES AND CONTRACTORS, AND COVERED NON-AGENCY PERSONNEL

(1) All material proposed for publication or public dissemination must be submitted to the PRB Chair, as described in paragraph d(1) above. The PRB Chair will have the responsibility for the review, coordination, and formal approval in writing of submissions in coordination with appropriate Board members. The PRB Chair will provide copies of submitted material to all components with equities in such material, and will also provide copies to all Board members and, upon request, to any Directorate-level Information Review Officer.

(2) The PRB will review material proposed for publication or public dissemination solely to determine whether it contains any classified information. Permission to publish will not be denied solely because the material may be embarrassing to or critical of the Agency. Former employees, contractors, or non-Agency personnel must obtain the written approval of the PRB prior to publication.

(3) When it is contemplated that a co-author who has not signed a CIA secrecy agreement will contribute to a publication subject to prepublication review, the final version of the publication must clearly identify those portions of the publication that were authored by the individual subject to the secrecy agreement. Where there is any ambiguity concerning which individual wrote a section, and the section was not submitted for review, the Agency reserves the right to

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
Approved for Release: 2017/04/06 C06652547

UNCLASSIFIED//~~AWO~~

consider the section to be entirely written by the individual subject to the secrecy agreement and therefore in violation of the individual's prepublication review obligations.

- (4) When otherwise classified information is also available independently in open sources and can be cited by the author, the PRB will consider the fact in making its determination on whether that information may be published with the appropriate citations. Nevertheless, the Agency retains the right to disallow certain open-source information or citations where, because of the author's Agency affiliation or position, the reference might confirm the classified content.

g. (U//~~AWO~~) PREPUBLICATION REVIEW GUIDELINES FOR CURRENT EMPLOYEES AND CONTRACTORS

- (1) All covered material proposed for publication or public dissemination must be submitted to the PRB Chair, as described in paragraph d(2) above. The PRB Chair will have the responsibility for the review, coordination, and formal approval in writing of submissions in coordination with the author's supervisor and other offices as necessary. The PRB Chair will provide copies of submitted material to all components with equities in such material, and will also provide copies to all Board members and, upon request, to any Directorate-level Information Review Officer.

- (2) Additional Review Criteria. Appropriateness. For current employees and contractors, in addition to the prohibition on revealing classified information, the Agency is also legally authorized to deny permission to publish any official or nonofficial materials on matters set forth in paragraphs e(1) and e(4) above that could:

- (a) reasonably be expected to impair the author's performance of his or her job duties,
- (b) interfere with the authorized functions of the CIA, or
- (c) have an adverse effect on the foreign relations or security of the United States.

These additional review criteria ensure that material is not published that could adversely affect the Agency's ability to function as an employer and carry out its national security mission. Because these criteria principally concern the Agency's authority as an employer to promote an effective work place and to protect the integrity of its mission, they apply only to the submissions of current CIA employees and contractors.

When a current CIA officer engages in public discussion of internal organizational operations, policies, and information, it could in certain circumstances interfere with CIA's ability, as an employer, to promote an effective work place and carry out its mission. When a current CIA officer engages in public discussion of current foreign relations issues or intelligence-related matters, it could in certain circumstances provide a factual basis for some to reasonably question whether the CIA was properly carrying out its independent, objective, and apolitical intelligence functions.

The determination of whether any particular publication could impair the author's performance of his or her duties, interfere with authorized CIA functions, or adversely affect the foreign relations or security of the United States must be assessed case-by-case in terms of the content of the manuscript, as well as the overall context and prevailing circumstances, including but not limited to, consideration of the currency of the subject matter; whether the subject matter is a matter of public concern; the degree

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
 Approved for Release: 2017/04/06 C06652547

UNCLASSIFIED//~~AWO~~

to which the topic is related to the author's official duties; whether the material submitted for review is required for a course at an accredited U.S. educational institution at any academic level and, if so, whether distribution is intended to extend beyond classroom use; and whether, in light of the assignment in which the author serves, the inclusion or exclusion of the disclaimer described in paragraph b(4) above can mitigate any concerns. The Agency will exercise its authority to deny permission to publish on the basis of any such determination only when the determination is made in writing and clearly identifies or describes how publication could create a significant risk of impairing the author's performance of his or her job duties, interfering with the authorized functions of the CIA, or adversely affecting the foreign relations or security of the United States.

Prior to drafting a manuscript intended for nonofficial publication, current CIA officers are encouraged to consult with the Board regarding the proposed topic or subject matter. In addition, current CIA officers must comply with any applicable component policies and procedures relating to consultation with management prior to the drafting of a manuscript, prior to submitting a manuscript to the Board, or during the prepublication review process. Any consultation with the Board or management may not necessarily result in Agency approval to publish the submitted manuscript.

- (3) Outside Activities Approval Request. Current employees and contractors must also complete a Form 879 (Outside Activity Approval Request) in accordance with Agency Regulation 10-15.

(4) Review Process:

- (a) Nonofficial publications. For all nonofficial publications, current employees must complete and submit to the PRB a cover memorandum identifying their immediate supervisor or contracting officer. The PRB will notify these individuals, whose concurrence is necessary for publication.
 - (b) Unclassified official publications. For all unclassified official publications that are covered by this regulation, current employees or contractors must first coordinate the document or speech with their management chain. Once initial management acceptance has been made, the employee must then submit the **proposed** publication to the PRB for final review and approval. (*Classified* official publications are not covered by this regulation and, therefore, are not required to be submitted to the PRB for review.)
 - (c) Resumes. This requirement for management review and concurrence does not apply for resumes, which must be sent to the PRB, which will coordinate their approval with the appropriate equity-owning component and Directorate-level Information Review Officer. The employee must obtain the written approval of the PRB prior to any dissemination of the resume outside of the CIA.
- (5) OGC Ethics Review for Executive Branch Employees. As part of the prepublication review process, and after PRB/management review of proposed publications is completed, the PRB will initiate a further review by OGC/Ethics Law Division (**OGC/ELD**) to determine if any ethics issues are raised under the *Standards of Ethical Conduct for Employees of the Executive Branch*. These Government-wide regulations and Agency Regulation 13-2 limit the use of nonpublic information and provide that an employee shall not receive compensation from any source other than the Government for teaching, speaking, or writing relating to the

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
 Approved for Release: 2017/04/06 C06652547

UNCLASSIFIED//~~AWO~~

employee's official duties. Additionally, OGC/ELD will also review proposed publications by current employees to ensure there is no violation of the criminal statute, 18 U.S.C. section 209, which prohibits an employee from receiving any salary or any contribution to or supplementation of salary from any source other than the U.S. as compensation for services as a Government employee. Specifically, employees may not receive outside compensation for any article, speech, or book written or produced as part of their official duties.

h. (U//~~AWO~~) APPEALS

- (1) If the PRB denies all or part of a proposed nonofficial publication, the author may submit additional material in support of publication and request reconsideration by the PRB. In the event the PRB denies the request for reconsideration, the author may appeal. PRB decisions involving nonofficial publications may be appealed to the ADD/CIA within 30 days of the decision. Such an appeal must be in writing and must be sent to the PRB Chair. Appeal documentation must include the material intended for publication and any supporting materials the appealing party wishes the ADD/CIA to consider. The PRB Chair will forward the appeal and relevant documentation through the components that objected to publication of the writing or other product at issue. The Director or Head of Independent Office will affirm or recommend revision of the decision affecting his or her component's equities and will forward that recommendation to OGC. OGC will review the recommendations for legal sufficiency and will make a recommendation to the ADD/CIA for a final Agency decision. The PRB Chair is responsible for staff support to the ADD/CIA. The ADD/CIA will render a written final decision on the appeal. Best efforts will be made to complete the appeal process within 30 days from the date the appeal is submitted.
- (2) This regulation is intended to provide direction and guidance for those persons who have prepublication review obligations and those who review material submitted for nonofficial or official publication. Nothing contained in this regulation or in any practice or procedure that implements this regulation is intended to confer, or does confer, any substantive or procedural right of privilege on any person or organization beyond that expressly stated herein.

- i. (U//~~AWO~~) BREACH OF SECRECY AGREEMENT. Failure to comply with prepublication review obligations can result in the imposition of civil penalties or damages. When the PRB becomes aware of a potential violation of the CIA secrecy agreement, it will notify OGC and the Office of Security (OS). After the OS review and investigation of the case is completed, if further action is deemed warranted, the OS will refer the matter to OGC, which will report all potentially criminal conduct to the Department of Justice (DoJ) and consult with DoJ regarding any civil remedies that may be pursued.

EXHIBIT B:

*Keeping Secrets Safe: The
Publications Review Board,
CIA*

(last updated Nov. 1, 2018)



**CENTRAL
INTELLIGENCE
AGENCY**

THE WORK OF A NATION.
THE CENTER OF INTELLIGENCE.

[Report Information](#)

[Contact](#)

Search CIA.gov...

[SEARCH](#)

عربي 中文 Français Русский Español [More](#) ▶

[HOME](#)

[ABOUT CIA](#)

[CAREERS & INTERNSHIPS](#)

[OFFICES OF CIA](#)

[NEWS & INFORMATION](#)

[LIBRARY](#)

[KIDS' ZONE](#)

About CIA

[About CIA](#)

[Today's CIA](#)

[Leadership](#)

[CIA Vision, Mission,
Ethos & Challenges](#)

[Headquarters Tour](#)

[CIA Museum](#)

[History of the CIA](#)

★ [Publications
Review Board](#)

[Accessibility](#)

[Privacy and Civil
Liberties](#)

[FAQs](#)

[No FEAR Act](#)

[Site Policies](#)

[Home](#) » [About CIA](#) » [Publications Review Board](#)

Keeping Secrets Safe: The Publications Review Board

All CIA officers, as a condition of employment, sign the standard CIA secrecy agreement when entering on duty. All contractors sign a secrecy agreement that is consistent with the terms and conditions of their contract. A secrecy agreement doesn't oblige officers and contractors to absolute silence, but it does require them to keep national security secrets for as long as the US Government deems the information to be classified. This is a lifelong obligation. In order to help avoid the damage to national security and to the Agency's mission that disclosing classified information would inflict, the CIA created the Publications Review Board (PRB) to preview materials produced by CIA personnel—former and current (both employees and contractors)—to determine if they contain such classified information before they are shared with publishers, blog-subscribers, a TV audience, ghost-writers, co-authors, editors, family members, assistants, representatives, or anyone else not authorized to receive or review such classified information.

What Must Be Submitted to the PRB?

Current and former CIA officers and contractors who have signed the standard CIA secrecy agreement are required to submit to the PRB any and all materials they intend to share with the public that are intelligence related, such as materials that mention the CIA or intelligence activities, or that concern topics to which they had access to classified information while employed at or performing contractual work for CIA. This submission requirement extends beyond the sub-set of topics they may have had immediate responsibility for on a day-to-day basis.

Publishing: Publishing is more than having a printing house bind copies of a book. It means communicating by any means (including orally or electronically), information regardless of form to any person or entity other than the CIA's PRB or a US Government official authorized by the CIA to receive such information for prepublication review. This encompasses materials including but not limited to: book reviews, Op-ed pieces, scholarly papers, scripts, screenplays, blogs, speeches, and other materials. Thus, material covered by a CIA Secrecy Agreement requiring prepublication review must be submitted and approved prior to discussing the material with or showing it to individuals such as a publisher, co-author, agent, editor, ghost-writer, personal representative, family member, or assistant.

Relating to CIA or intelligence activities: Not everything former and current CIA officers and contractors write requires prepublication review. For example, the prepublication requirement does not apply to material such as gardening, wine tasting, stamp collecting, sports and so forth, because they are outside of the purview of the CIA mission or intelligence. However, commentary on matters such as intelligence operations or tradecraft (even fictional works), foreign intelligence, foreign events of intelligence interest, one's career, scientific or technological developments discussed in an intelligence context, and other topics that touch upon CIA interests or responsibilities need PRB approval.

Why Do Materials Need To Be Reviewed?

In addition to protecting national security, the PRB is also protecting CIA officers and contractors from legal liability. For instance, one may unwittingly share insights on events and capabilities that are thought to be public knowledge, but in fact have not been officially released by the CIA or the US Government. Accidental disclosure is still disclosure, and opens a person up to possible civil or criminal penalties. The PRB helps current and former CIA officers and contractors avoid this by identifying problematic material and working with them to find ways to make their points, while avoiding classified information disclosure. For instance, PRB staff often compare declassified material found at the CIA's [FOIA Reading Room](#) and [CIA.gov](#) with materials submitted for review.

ABOUT CIA



Headquarters Tour

Take a look inside the CIA.



Interactive Timeline

Experience more than 60 years of CIA history.

[Learn More About CIA](#)

CONNECT WITH CIA



TWITTER FEED

Tweets by @CIA



CIA
@CIA

Replying to @CIA

A good place to start learning about CIA is our website. There's lots of great info hidden in the nooks & crannies. Poke around & see what you can find.

Whatever career path you decide on, good luck in all your endeavors.

[Embed](#)

[View on Twitter](#)

[View @CIA Twitter Feed](#)

What Kind of Information Might Be Classified?

As outlined in [Executive Order 13526](#) (sec. 1.4), the following categories of information may be classified if unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security:

- military plans, weapons systems, or operations;
- foreign government information;
- intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- foreign relations or foreign activities of the United States, including confidential sources;
- scientific, technological, or economic matters relating to the national security;
- United States Government programs for safeguarding nuclear materials or facilities;
- vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
- the development, production, or use of weapons of mass destruction.

In combination with these criteria, authors are encouraged to ask the following questions during the writing process to get an idea of what information the PRB is protecting:

"As worded, does the text reveal classified information? Why is this information classified [or not]?"

"Would releasing this information damage national security or harm CIA's intelligence sources and methods?"

Some individual pieces of information may not cause national security damage when standing alone, but can do so if compiled with other information. Also, the PRB is not authorized to release official records or text from Government documents. Individuals seeking such information may submit a FOIA or Privacy Act Request using the procedures found [here](#) and [here](#), respectively.

Resume Prepublication Review

One of the challenges of a career in intelligence is composing a resume that doesn't reveal any secrets. Although many details of the Agency's work are classified, a lot of information about [CIA jobs](#) are publicly available. These occupational descriptions are great examples of what current and former Agency officers can share about their work, and provide a good basis on which to prepare resumes and memoirs that will smoothly pass through the prepublication review process. In addition, the guidelines below may be generally helpful for avoiding content that is problematic for prepublication review. Remember – some things CANNOT be used:

- **Countries** - Use regional terms instead of specific cities or countries.
- **Agency-specific** - Use general training or software descriptions as opposed to the specific names or titles, which may be classified.
- **Names** - Do not use names of people and/or places. Please contact the Publications Review Board before using Agency colleagues as references.
- **Numbers** - Use general terms to describe budget information and/or personnel information (e.g., "hundreds" or "millions" or "several")
- **Office** - Do not use organizational names below the office level (e.g., avoid group or branch names).
- **Technical details** - Use general terms instead of the specific details.

How To Reach Us?

The PRB exists to help protect against unauthorized disclosures, but ultimately, each CIA officer or contractor is responsible for protecting any classified information they possess. Should a CIA officer or contractor publish materials that contain classified information – either because they did not comply with the PRB's changes or because they chose to bypass the PRB process by not submitting their manuscript for PRB pre-publication review – they could be subject to possible civil and criminal penalties. Cooperating with pre-publication review helps keep CIA officers, contractors, and the Agency safe.

Former Agency officers and contractors who need to contact the PRB regarding items to be reviewed can do so through the [Contact CIA](#) page. (If using the web form, please be sure to fill out the form completely, including your full legal name and email address where you can be reached).



About CIA

[Today's CIA](#)
[Leadership](#)
[CIA Vision, Mission, Ethos & Challenges](#)
[Headquarters Tour](#)
[CIA Museum](#)
[History of the CIA](#)
[Publications Review Board](#)
[Accessibility](#)
[Privacy and Civil Liberties](#)
[FAQs](#)
[No FEAR Act](#)
[Site Policies](#)

Careers & Internships

[Career Opportunities](#)
[Language Opportunities](#)
[Application Process](#)
[Life at CIA](#)
[Benefits](#)
[Diversity](#)
[Military Transition](#)
[Tools and Challenges](#)
[FAQs](#)
[Video Center](#)

Offices of CIA

[Intelligence & Analysis](#)
[Clandestine Service](#)
[Science & Technology](#)
[Support to Mission](#)
[Digital Innovation](#)
[Mission Centers](#)
[Human Resources](#)
[Public Affairs](#)
[General Counsel](#)
[Equal Employment Opportunity](#)
[Congressional Affairs](#)
[Inspector General](#)
[Military Affairs](#)

News & Information

[Blog](#)
[Press Releases & Statements](#)
[Speeches & Testimony](#)
[CIA & the War on Terrorism](#)
[Featured Story Archive](#)
[Your News](#)

Library

[Publications](#)
[Center for the Study of Intelligence](#)
[Freedom of Information Act](#)
[Electronic Reading Room](#)
[Kent Center Occasional Papers](#)
[Intelligence Literature](#)
[Reports](#)
[Related Links](#)
[Video Center](#)

Kids' Zone

[K-5th Grade](#)
[6-12th Grade](#)
[Parents & Teachers](#)
[Games](#)
[Related Links](#)
[Privacy Statement](#)

Connect with CIA



* REQUIRED PLUGINS [Adobe® Reader®]

EXHIBIT C:

DD Form 1847-1, *Sensitive
Compartmented Information
Nondisclosure Statement*
(Dec. 1991)

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE STATEMENT**PRIVACY ACT STATEMENT**

AUTHORITY: EO 9397, November 1943 (SSN).

PRINCIPAL PURPOSE(S): The information contained herein will be used to precisely identify individuals when it is necessary to certify their access to sensitive compartmented information.

ROUTINE USE(S): Blanket routine uses, as published by Defense Intelligence Agency in the Federal Register.

DISCLOSURE: Voluntary; however, failure to provide requested information may result in delaying the processing of your certification.

SECTION A

An Agreement Between _____ and the United States.
(Printed or Typed Name)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or in the process of a classification determination under the standards of Executive Order 12356 or other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. I have been advised that unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be SCI, or related to or derived from SCI, is considered by such Department or Agency to be SCI. I further understand that I am also obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.

4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I

4. (Continued) have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation to any person not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.

5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 set forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon them, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.

6. I have been advised that any breach of this Agreement may result in the termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including the provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys' fees incurred by the United States Government may be assessed against me if I lose such action.

8. I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a

| | | | |
|---|--|--------------------------------|---|
| <p>8. <i>(Continued)</i> court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code.</p> <p>9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all the conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.</p> <p>10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.</p> <p>11. These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations, rights, or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act</p> | <p>11. <i>(Continued)</i> (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Section 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.</p> <p>12. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798, and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 12356, as amended, so that I may read them at this time, if I so choose.</p> <p>13. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.</p> <p>14. This Agreement shall be interpreted under and in conformance with the laws of the United States.</p> <p>15. I make this Agreement without any mental reservation or purpose of evasion.</p> | | |
| 16. TYPED OR PRINTED NAME <i>(Last, First, Middle Initial)</i> | 17. GRADE/RANK/SVC | 18. SOCIAL SECURITY NO. | 19. BILLET NO. <i>(Optional)</i> |
| 20. ORGANIZATION | 21. SIGNATURE | | 22. DATE SIGNED <i>(YYMMDD)</i> |
| FOR USE BY MILITARY AND GOVERNMENT CIVILIAN PERSONNEL | | | |
| SECTION B | | | |
| The execution of this Agreement was witnessed by the undersigned, who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information. | | | |
| 23. TYPED OR PRINTED NAME <i>(Last, First, Middle Initial)</i> | | 24. ORGANIZATION | |
| 25. SIGNATURE | | | 26. DATE SIGNED <i>(YYMMDD)</i> |
| FOR USE BY CONTRACTORS/CONSULTANTS/NON-GOVERNMENT PERSONNEL | | | |
| SECTION C | | | |
| The execution of this Agreement was witnessed by the undersigned. | | | |
| 27. TYPED OR PRINTED NAME <i>(Last, First, Middle Initial)</i> | | 28. ORGANIZATION | |
| 29. SIGNATURE | | | 30. DATE SIGNED <i>(YYMMDD)</i> |
| SECTION D | | | |
| This Agreement was accepted by the undersigned on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information. | | | |
| 31. TYPED OR PRINTED NAME <i>(Last, First, Middle Initial)</i> | | 32. ORGANIZATION | |
| 33. SIGNATURE | | | 34. DATE SIGNED <i>(YYMMDD)</i> |

EXHIBIT D:

DoD Directive 5230.09,
*Clearance of DoD Information
for Public Release*
(Apr. 14, 2017)



Department of Defense **DIRECTIVE**

NUMBER 5230.09

August 22, 2008

Certified Current Through August 22, 2015

Incorporating Change 2, April 14, 2017

DCMO

SUBJECT: Clearance of DoD Information for Public Release

References: See Enclosure 1

1. PURPOSE. This Directive reissues DoD Directive (DoDD) 5230.09 (Reference (a)) to update policy and responsibilities for the security and policy review process for the clearance of official DoD information proposed for official public release by the Department of Defense and its employees under DoDD 5105.02 (Reference (b)).

2. APPLICABILITY AND SCOPE

a. This Directive applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

(2) All DoD personnel.

b. This Directive does NOT apply for provisions governing review of:

(1) Prepared statements, transcripts of testimony, questions for the record, inserts for the record, budget documents, and other material provided to congressional committees that may be included in the published records. (DoD Instruction (DoDI) 5400.04 (Reference (c)) applies.)

(2) Information before publication or disclosure by DoD contractors. (DoD 5220.22-M and DoD Manual 5200.01 (References (d) and (e)) apply.)

(3) Official information in litigation. (DoDD 5405.2 (Reference (f)) applies.)

(4) Release of official DoD information to the news media. (DoDD 5122.05 (Reference (g)) applies.)

3. DEFINITIONS. Terms used in this Directive are defined in the glossary.

4. POLICY. It is DoD policy that:

a. Accurate and timely information is made available to the public and the Congress to help the analysis and understanding of defense strategy, defense policy, and national security issues.

b. Any official DoD information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the Department of Defense shall be reviewed for clearance prior to release.

c. The public release of official DoD information is limited only as necessary to safeguard information requiring protection in the interest of national security or other legitimate governmental interest, as authorized by References (e), (f), and (g) and DoDDs ~~5230.24~~, 5230.25, 5400.07, 5400.11, 5205.02E, and 5500.07; DoDI ~~s~~ 5230.27, ~~5230.24~~, and ~~DoDI~~ 5200.01; DoD *Manual* 5400.07-~~R~~; DoD 5400.11-R; DoD 5500.7-R; International Traffic in Arms Regulations; Executive Order 13526; section 4353 of Title 22, United States Code (U.S.C.); and Executive Order 13556 (References (h) through (v), respectively).

d. Information released officially is consistent with established national and DoD policies and programs, including DoD Information Quality Guidelines (Reference (w)).

e. To ensure a climate of academic freedom and to encourage intellectual expression, students and faculty members of an academy, college, university, or DoD school are not required to submit papers or materials prepared in response to academic requirements for review when they are not intended for release outside the academic institution. Information intended for public release or made available in libraries to which the public has access shall be submitted for review. Clearance shall be granted if classified information is not disclosed, DoD interests are not jeopardized, and the author accurately portrays official policy, even if the author takes issue with that policy.

f. Retired personnel, former DoD employees, and non-active duty members of the Reserve Components shall use the DoD security review process to ensure that information they submit for public release does not compromise national security.

g. DoD personnel, while acting in a private capacity and not in connection with their official duties, have the right to prepare information for public release through non-DoD fora or media. This information must be reviewed for clearance if it meets the criteria in DoDI 5230.29 (Reference (x)). Such activity must comply with ethical standards in References (q) and (r) and may not have an adverse effect on duty performance or the authorized functions of the Department of Defense.

5. RESPONSIBILITIES. See Enclosure 2.
6. RELEASABILITY. **Cleared for public release.** This Directive is available on the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.
7. EFFECTIVE DATE. This Directive is effective February 22, 2012.



Gordon England
Deputy Secretary of Defense

Enclosures

1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5230.9, "Clearance of Department of Defense (DoD) Information for Public Release," April 9, 1996 (hereby canceled)
- (b) DoD Directive 5105.02, "Deputy Secretary of Defense," February 18, 2015
- (c) DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009
- (d) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended
- (e) DoD Manual 5200.01, "DoD Information Security Program," February 24, 2012, ~~as amended~~ *date varies by volume*
- (f) DoD Directive 5405.2, "Release of Official Information in Litigation and Testimony by DoD Personnel as Witnesses," July 23, 1985
- (g) DoD Directive 5122.05, "Assistant Secretary of Defense for Public Affairs (ASD(PA))," September 5, 2008
- (h) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," ~~October 9, 2008, as amended~~ *April 21, 2016*
- (i) DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, *as amended*
- (j) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984, as amended
- (k) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," ~~October 6, 1987~~ *November 18, 2016*
- (l) DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 2, 2008
- (m) DoD ~~Manual~~ 5400.07-R, "DoD Freedom of Information Act (*FOIA*) Program," ~~September 4, 1998~~ *January 25, 2017*
- (n) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
- (o) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (p) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012
- (q) DoD Directive 5500.07, "Standards of Conduct," November 29, 2007
- (r) DoD 5500.07-R, "Joint Ethics Regulation (JER)," August 1, 1993, as amended
- (s) International Traffic in Arms Regulations (ITAR), Department of State, current edition
- (t) Executive Order 13526, "Classified National Security Information," December 29, 2009
- (u) Section 4353 of Title 22, United States Code
- (v) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
- (w) DoD Information Quality Guidelines, current edition¹
- (x) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014
- (y) DoD Directive 5105.53, "Director of Administration and Management (DA&M)," February 26, 2008

¹ Available at www.defensegov/pubs/dodiqguidelines.aspx.

- (z) DoD Directive 5105.82, "Deputy Chief Management Officer (DCMO) of the Department of Defense," October 17, 2008
- (aa) Deputy Secretary of Defense Memorandum, "Reorganization of the Office of the Deputy Chief Management Officer," July 11, 2014
- (ab) DoD Directive 5110.04, "Washington Headquarters Services (WHS)," March 27, 2013
- (ac) Title 10, United States Code

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR OF ADMINISTRATION OF THE OFFICE OF THE DEPUTY CHIEF MANAGEMENT OFFICER (DCMO) OF THE DEPARTMENT OF DEFENSE-~~(DCMO)~~.

Under the authority, direction, and control of the DCMO, and in accordance with DoDD 5105.53, DoDD 5105.82, and Deputy Secretary of Defense Memorandum (References (y), (z), and (aa)), the Director of Administration of the Office of the DCMO acts as the appellate authority for the DoD security and policy review process.

2. DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (WHS). Under the authority, direction, and control of the DCMO and through the Director of Administration of the Office of the DCMO, the Director, WHS:

- a. Monitors compliance with this Directive.
- b. Develops procedures and review guidelines for the security and policy review of information intended for public release in coordination with offices of the OSD Principal Staff Assistants.
- c. Implements the DoD security review process through the Defense Office of Prepublication and Security Review (DOPSR) in accordance with DoDD 5110.04 (Reference (ab)).

3. INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE. The Inspector General of the Department of Defense, as an independent and objective officer in the Department of Defense, is exempt from the policy review provisions of this Directive. As necessary, information may be submitted for security review prior to public release.

4. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

- a. Provide prompt guidance and assistance to the Director, WHS, when requested, for the security or policy implications of information proposed for public release.
- b. Establish policies and procedures to implement this Directive in their Components. Designate the DoD Component office and point of contact for implementation of this Directive and provide this information to the DOPSR.
- c. Forward official DoD information proposed for public release to the Director, WHS, for review, including a recommendation on the releasability of the information per Reference (x).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

| | |
|--------|---|
| DCMO | Deputy Chief Management Office of the Department of Defense |
| DoDD | DoD Directive |
| DoDI | DoD Instruction |
| DOPSR | Defense Office of Prepublication and Security Review |
| U.S.C. | United States Code |
| WHS | Washington Headquarters Services |

PART II. DEFINITIONS

The following terms and their definitions are for the purposes of this Directive only.

DoD personnel:

Any DoD civilian officer or employee (including special Government employees) of any DoD Component (including any nonappropriated fund activity).

Any active duty Regular or Reserve military officer, warrant officer, and active duty enlisted member of the Army, the Navy, the Air Force, or the Marine Corps.

Any Reserve or National Guard member on active duty under orders issued pursuant to Title 10, U.S.C. (Reference (ac)).

Any Reserve or National Guard member performing official duties, including while on inactive duty for training or while earning retirement points, pursuant to Reference (ac), or while engaged in any activity related to the performance of a Federal duty or function.

Any faculty member in a civil service position or hired pursuant to Reference (ac) and any student (including a cadet or midshipman) of an academy, college, university, or school of the Department of Defense.

Any foreign national working for a DoD Component except those hired pursuant to a defense contract, consistent with labor agreements, international treaties and agreements, and host-country laws.

information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form.

official DoD information. All information that is in the custody and control of the Department of Defense, relates to information in the custody and control of the Department, or was acquired by DoD employees as part of their official duties or because of their official status within the Department.

review for clearance. The process by which information that is proposed for public release is examined for compliance with established national and DoD policies and to determine that it contains no classified or export-controlled information. Release of information to the public, cleared by the DOPSR, is the responsibility of the originating office.

EXHIBIT E:

DoD Instruction 5230.09,
*Clearance of DoD Information
for Public Release*
(effective Jan. 25, 2019)



DoD INSTRUCTION 5230.09

CLEARANCE OF DoD INFORMATION FOR PUBLIC RELEASE

Originating Component: Office of the Chief Management Officer of the Department of Defense

Effective: January 25, 2019

Releasability: Cleared for public release. Available on the Directives Division Website at <http://www.esd.whs.mil/DD/>.

Reissues and Cancels: DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008, as amended

Approved by: Lisa W. Hershman, Acting Chief Management Officer

Purpose: This issuance reissues the 2008 directive as a DoD instruction in accordance with the authority in DoD Directive (DoDD) 5105.82 and the February 1, 2018 Secretary of Defense Memorandum to establish policy and assign responsibilities for the security and policy review process for the clearance of official DoD information proposed for official public release by the DoD and its employee.

DoDI 5230.09, January 25, 2019

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION 3

 1.1. Applicability. 3

 1.2. Policy. 3

SECTION 2: RESPONSIBILITIES 5

 2.1. Director of Administration of the Office of the Chief Management Officer of the
 Department of Defense (OCMO)..... 5

 2.2. Director, Washington Headquarters Services (WHS). 5

 2.3. DoD Component Heads. 5

GLOSSARY 6

 G.1. Acronyms. 6

 G.2. Definitions..... 6

REFERENCES 8

DoDI 5230.09, January 25, 2019

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the “DoD Components”).

b. This issuance does not apply for provisions governing review of:

(1) Prepared statements, transcripts of testimony, questions for the record, inserts for the record, budget documents, and other material provided to congressional committees that may be included in the published records in accordance with DoD Instruction (DoDI) 5400.04.

(2) Information before publication or disclosure by DoD contractors in accordance with DoD 5220.22-M and Volumes 1-4 of DoD Manual (DoDM) 5200.01.

(3) Official information in litigation in accordance with DoDD 5405.2.

(4) Release of official DoD information to media organizations in accordance with DoDD 5122.05.

(5) Release of visual imagery, captured by DoD personnel on personal equipment, to media organizations in accordance with DoDI 5040.02.

(6) Release of information requested pursuant to Section 552 of Title 10, United States Code (U.S.C.) (also known as “the Freedom of Information Act”) and Section 552 of Title 10, U.S.C. (also known as “the Privacy Act”).

1.2. POLICY. It is DoD policy that:

a. Accurate and timely information is made available to the public and the Congress to help with analysis and understanding of defense strategy, defense policy, and national security issues.

b. Any official DoD information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the DoD will undergo a prepublication review before release.

c. The Office of the Inspector General of the Department of Defense, as an independent and objective component in the DoD, is exempt from the policy review provisions of this issuance. As necessary, information may be submitted for prepublication review before public release.

d. The public release of official DoD information is limited only as necessary to safeguard information requiring protection in the interest of national security or other legitimate

DoDI 5230.09, January 25, 2019

governmental interest, as authorized by DoDDs 5122.05, 5205.02E, 5230.25, 5400.07, 5400.11, 5405.2, and 5500.07; DoDIs 5200.01, 5230.24, and 5230.27; Volumes 1-4 of DoDM 5200.01 and DoDM 5400.07; DoD 5400.11-R; DoD 5500.07-R; Chapter I, Subchapter M, Parts 120 through 130 of Title 22, Code of Federal Regulations; Executive Orders 13526 and 13556; and Section 4353 of Title 22, U.S.C.

e. Information released officially is consistent with established national and DoD policies and programs.

f. To ensure a climate of academic freedom and to encourage intellectual expression, DoD personnel who are students or faculty members of an academy, college, university, or DoD school:

(1) Are not required to submit for prepublication review papers or materials prepared in response to academic requirements when they are not intended for release outside the academic institution. However, these individuals remain obligated to ensure their work contains no classified, sensitive or controlled unclassified sources consistent with their nondisclosure agreements.

(2) Will submit materials for prepublication review if they are intended for public release or will be made available in public libraries. Clearance will be granted if classified information is not disclosed, controlled unclassified information is not disclosed, DoD interests are not jeopardized, and the author accurately portrays official policy, even if the author takes issue with that policy.

g. Retired and separated Service members, former DoD employees and contractors, and non-active duty members of the Reserve Components will use the DoD prepublication review process to ensure that information they intend to release to the public does not compromise national security as required by their nondisclosure agreements. Those who forgo the prepublication review process and inadvertently, negligently, or willfully disclose classified information may be subject to an unauthorized disclosure investigation and legal action.

h. DoD personnel, while acting in a private capacity and not in connection with their official duties, may prepare information for public release through non-DoD venues or media. This information must undergo a prepublication review if it meets the criteria in DoDI 5230.29. Such activity must comply with ethical standards in DoDD 5500.07 and DoD 5500.07-R and may not have an adverse effect on duty performance or the authorized functions of the DoD.

DoDI 5230.09, January 25, 2019

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR OF ADMINISTRATION OF THE OFFICE OF THE CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE (OCMO). Under the authority, direction, and control of the Chief Management Officer of the Department of Defense and in accordance with DoDD 5105.53, DoDD 5105.82, and the July 11, 2014 and February 1, 2018 Deputy Secretary of Defense memorandums, the Director of Administration of the OCMO acts as the appellate authority for the DoD security and policy review process.

2.2. DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (WHS). Under the authority, direction, and control of the Chief Management Officer of the Department of Defense and through the Director of Administration of the OCMO, the Director, WHS:

- a. Monitors compliance with this issuance.
- b. Develops procedures and reviews guidelines for the security and policy review of information intended for public release in coordination with offices of the OSD Principal Staff Assistants.
- c. Implements the DoD prepublication review process through the Defense Office of Prepublication and Security Review in accordance with DoDD 5110.04.

2.3. DOD COMPONENT HEADS. The DoD Component heads:

- a. Provide prompt guidance and assistance to the Director, WHS, when requested, for the security or policy implications of information proposed for public release.
- b. Establish policies and procedures to implement this issuance in their Components. Designate the DoD Component office and point of contact for implementation of this issuance and provide this information to the Defense Office of Prepublication and Security Review.
- c. Forward official DoD information proposed for public release to the Director, WHS, for review, including a recommendation on the releasability of the information in accordance with DoDI 5230.29.

DoDI 5230.09, January 25, 2019

GLOSSARY

G.1. ACRONYMS.

| | |
|--------|---|
| DoDD | DoD directive |
| DoDI | DoD instruction |
| DoDM | DoD manual |
| OCMO | Office of the Chief Management Officer of the Department of Defense |
| U.S.C. | United States Code |
| WHS | Washington Headquarters Services |

G.2. DEFINITIONS. These terms and their definitions are for the purpose of this issuance.

DoD personnel.

Any DoD civilian officer or employee (including special government employees) of any DoD Component (including any nonappropriated fund activity).

Any individual hired by or for any DoD Component through a contractual arrangement.

Any active duty Regular or Reserve military officer, warrant officer, and active duty enlisted member of the Military Services.

Any Reserve or National Guard member on active duty under orders issued pursuant to Title 10, U.S.C.

Any Reserve or National Guard member performing official duties, including while on inactive duty for training or while earning retirement points, pursuant to Title 10, U.S.C., or while engaged in any activity related to the performance of a federal duty or function.

Any faculty member in a civil service position or hired pursuant to Title 10, U.S.C. and any student (including a cadet or midshipman) of an academy, college, university, or school of the DoD.

Any foreign national working for a DoD Component consistent with labor agreements, international treaties and agreements, and host-country laws.

information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form.

official DoD information. All information that is in the custody and control of the DoD, relates to information in the custody and control of the DoD, or was acquired by DoD personnel as part of their official duties or because of their official status within DoD.

DoDI 5230.09, January 25, 2019

prepublication review. The process by which information that is proposed for public release is examined by the Defense Office of Prepublication and Security Review for compliance with established national and DoD policies and to determine whether it contains any classified, export-controlled or other protected information. It is the responsibility of the originating office to ensure that this prepublication review is followed and that clearance is granted prior to the release of the information to the public.

DoDI 5230.09, January 25, 2019

REFERENCES

- Code of Federal Regulations, Title 22, Chapter I, Subchapter M, Parts 120 through 130
- Deputy Secretary of Defense Memorandum, "Reorganization of the Office of the Deputy Chief Management Officer," July 11, 2014
- Deputy Secretary of Defense Memorandum, "Disestablishment of the Deputy Chief Management Officer and Establishment of the Chief Management Officer," February 1, 2018
- DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended
- DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- DoD 5500.07-R, "Joint Ethics Regulation (JER)," August 30, 1993, as amended
- DoD Directive 5105.53, "Director of Administration and Management (DA&M)," February 26, 2008
- DoD Directive 5105.82, "Deputy Chief Management Officer (DCMO) of the Department of Defense," October 17, 2008
- DoD Directive 5110.04, "Washington Headquarters Services (WHS)," March 27, 2013
- DoD Directive 5122.05, "Assistant To the Secretary of Defense for Public Affairs (ATSD(PA))," August 7, 2017
- DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012
- DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984, as amended
- DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 2, 2008
- DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
- DoD Directive 5405.2, "Release of Official Information in Litigation and Testimony by DoD Personnel as Witnesses," July 23, 1985
- DoD Directive 5500.07, "Standards of Conduct," November 29, 2007
- DoD Instruction 5040.02, "Visual Information (VI)," October 27, 2011, as amended
- DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016
- DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, as amended
- DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," November 18, 2016, as amended
- DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended
- DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009
- DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012
- DoD Manual 5200.01, Volume 2, "DoD Information Security Program: DoD Information Security Program: Marking Of Classified Information," February 24, 2012, as amended

DoDI 5230.09, January 25, 2019

DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection Of Classified Information," February 24, 2012, as amended
DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012
DoD Manual 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 25, 2017
Executive Order 13526, "Classified National Security Information," December 29, 2009
Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
Secretary of Defense Memorandum, "Disestablishment of the Deputy Chief Management Officer and Establishment of the Chief Management Officer," February 1, 2018
United States Code, Title 10
United States Code, Title 22, Section 4353

EXHIBIT F:

DoD Instruction 5230.29,
*Security and Policy Review of
DoD Information for Public
Release*

(Apr. 14, 2017)



Department of Defense INSTRUCTION

NUMBER 5230.29

August 13, 2014

Incorporating Change 1, April 14, 2017

DCMO

SUBJECT: Security and Policy Review of DoD Information for Public Release

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5105.53 (Reference (a)), *DoDD 5105.82 (Reference (b))*, and Deputy Secretary of Defense Memorandum (Reference (bc)), this instruction reissues DoD Instruction (DoDI) 5230.29 (Reference (ed)) to implement policy established in DoDD 5230.09 (Reference (de)), assigns responsibilities, and prescribes procedures to carry out security and policy review of DoD information for public release.
2. APPLICABILITY. This instruction:
 - a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").
 - b. Does not apply to the Office of the Inspector General of the Department of Defense. The Inspector General of the Department of Defense, as an independent and objective officer in the DoD, is exempt from the policy review provisions of this instruction. As necessary, information may be submitted for security review before public release.
3. POLICY. In accordance with Reference (de), it is DoD policy that a security and policy review will be performed on all official DoD information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the DoD.
4. RESPONSIBILITIES. See Enclosure 2.
5. PROCEDURES. Enclosure 3 contains clearance requirements, submission procedures, time limits, information concerning review determinations, and appeals.

DoDI 5230.29, August 13, 2014

6. RELEASABILITY. **Cleared for public release.** This instruction is available on the ~~Internet~~ ~~from the~~ DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

7. EFFECTIVE DATE. This instruction ~~is effective August 13, 2014.~~

~~a. Is effective August 13, 2014.~~

~~b. Will expire effective August 13, 2024 if it hasn't been reissued or cancelled before this date in accordance with DoDI 5025.01 (Reference (c)).~~



David Tillotson III
Assistant Deputy Chief Management Officer

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

DoDI 5230.29, August 13, 2014

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5105.53, "Director of Administration and Management (DA&M)," February 26, 2008
- (b) *DoD Directive 5105.82, "Deputy Chief Management Officer (DCMO) of the Department of Defense," October 17, 2008*
- (bc) Deputy Secretary of Defense Memorandum, "Reorganization of the Office of the Deputy Chief Management Officer," July 11, 2014
- (ed) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," January 8, 2009 (hereby cancelled)
- (de) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008, as amended
- ~~(e) DoD Instruction 5025.01, "DoD Issuances Program," June 6, 2014~~
- (f) DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009
- (g) DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, *as amended*
- (h) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984, as amended
- (i) Parts 120-130 of Title 22, Code of Federal Regulations (also known as "The International Traffic in Arms Regulations (ITAR)")
- (j) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012
- (k) DoD Manual 5200.01, "DoD Information Security Program," ~~February 24, 2012, as amended~~ *date varies by volume*
- (l) Deputy Secretary of Defense Memorandum, "Congressional Testimony Coordination and Clearance Procedures," January 17, 2012¹
- (m) DoD Instruction 2205.02, "Humanitarian and Civic Assistance (HCA) Activities," June 23, 2014
- (n) DoD Instruction 3000.05, "Stability Operations," September 16, 2009
- (o) DoD Directive 5122.05, "Assistant Secretary of Defense for Public Affairs (ASD(PA))," September 5, 2008
- (p) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
- (q) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," ~~October 6, 1987~~ *November 18, 2016*
- (r) DoD Instruction 3200.12, "DoD Scientific and Technical Information Program (STIP)," August 22, 2013
- (s) DoD Manual 3200.14, Volume 1, "Principles and Operational Parameters of the DoD Scientific and Technical Information Program (STIP): General Processes," March 14, 2014

¹ Available at <http://www.dtic.mil/whs/esd/osr>

DoDI 5230.29, August 13, 2014

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR OF ADMINISTRATION, OFFICE OF THE DEPUTY CHIEF MANAGEMENT OFFICER (DCMO) OF THE DEPARTMENT OF DEFENSE (DA ODCMO). Under the authority, direction, and control of the ~~Deputy Chief Management Officer (DCMO) of the Department of Defense~~, the ~~Director of Administration DA ODCMO~~ acts as the appellate authority for the DoD security and policy review process.

2. DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (WHS). Under the authority, direction, and control of the DCMO, through the ~~Director of Administration DA ODCMO~~, the Director, WHS:

a. Monitors compliance with the procedures established in Enclosure 3 of this instruction for the security and policy review of official DoD information.

b. Provides for the timely security and policy review of official DoD information proposed for public release that is originated by, in, or for the DoD, including statements intended for open presentation before the Congress and other material submitted to the Congress in accordance with DoDI 5400.04 (Reference (f)).

c. Provides for the timely policy review of official DoD information that is originated by the DoD for presentation before a closed session of the Congress and other classified material submitted to the Congress in accordance with Reference (f).

d. Coordinates, as necessary, with the DoD Component staffs when reviewing official DoD information for public release clearance to ensure accuracy and currency of existing policy and security guidance.

e. Responds to requests for review of information submitted by DoD personnel acting in a private capacity or submitted voluntarily by non-DoD sources to ensure that classified information is not disclosed. This review will also address technology transfer and public releasability of technical data in accordance with DoDI 5230.24, DoDD 5230.25, and parts 120 through 130 of Title 22, Code of Federal Regulations (References (g), (h), and (i)).

f. Supports other Executive Department and non-DoD agency security review programs in the release of information to the public that may contain DoD equities.

3. OSD AND DOD COMPONENT HEADS. The OSD and DoD Component heads:

a. Ensure Component compliance with this instruction, and issue any guidance necessary for the internal administration of the requirements prescribed in Enclosure 3 of this instruction.

DoDI 5230.29, August 13, 2014

b. Ensure prompt Component guidance and assistance to the Chief, Defense Office of Prepublication and Security Review (DOPSR), when requested, on any information proposed for public release.

c. Exercise Component clearance authority for information not specified in section 1 of Enclosure 3 of this instruction. This authority may be delegated to the lowest level competent to evaluate the content and implications of public release of the information.

d. Ensure that Component-specific documents, including official correspondence, are reviewed internally and that information not specified in Enclosure 3 of this instruction is reviewed for operations security and information security in accordance with DoDD 5205.02E and DoD Manual 5200.01 (References (j) and (k)) before public release. This review will also address technology transfer and public releasability of technical data in accordance with References (g), (h), and (i).

e. Ensure Component compliance with the guidelines of the Deputy Secretary of Defense Memorandum (Reference (l)) concerning the coordination and clearance process of Congressional testimony to facilitate timely security and policy review.

f. Ensure effective information sharing between the Component and designated mission partners in accordance with DoDI 2205.02 and DoDI 3000.05 (References (m) and (n)).

g. Ensure that Component release of DoD information to news media representatives is in accordance with DoDD 5122.05 (Reference (o)).

DoDI 5230.29, August 13, 2014

ENCLOSURE 3

PROCEDURES

1. CLEARANCE REQUIREMENTS. The security review protects classified information, controlled unclassified information, or unclassified information that may individually or in aggregate lead to the compromise of classified information or disclosure of operations security. The policy review ensures that no conflict exists with established policies or programs of the DoD or the U.S. Government. Official DoD information that is prepared by or for DoD personnel and is proposed for public release will be submitted for review and clearance if the information:

- a. Originates or is proposed for release in the National Capital Region by senior personnel (e.g., general or flag officers and Senior Executive Service) on sensitive political or military topics;
- b. Is or has the potential to become an item of national or international interest;
- c. Affects national security policy, foreign relations, or ongoing negotiations;
- d. Concerns a subject of potential controversy among the DoD Components or with other federal agencies;
- e. Is presented by a DoD employee who, by virtue of rank, position, or expertise, would be considered an official DoD spokesperson; or
- f. Contains technical data, including data developed under contract or independently developed and subject to potential control in accordance with Reference (i), that may be militarily critical (as defined in the Glossary) and subject to limited distribution, but on which a distribution determination has not been made.

2. SUBMISSION PROCEDURES

a. Detailed Procedures. These procedures apply to all information required to be submitted to DOPSR for clearance:

(1) A minimum of three hard copies of material, in its final form, will be submitted, together with a signed DD Form 1910, "Clearance Request for Public Release of Department of Defense Information," located at the DoD Forms Management Program website at <http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm>, to:

Chief, Defense Office of Prepublication and Security Review
1155 Defense Pentagon
Washington, D.C. 20301-1155

DoDI 5230.29, August 13, 2014

(2) If the material is fewer than 100 pages long, one soft copy of the unclassified material and the DD Form 1910 may be submitted by e-mail to whs.pentagon.esd.mbx.secrev@mail.mil instead of the requirements of paragraph 2a(1) of this enclosure.

(3) Any material submitted for review will be approved by an authorized government representative of the submitting office to indicate that office's approval of the material for public release. Contractors may not sign the DD Form 1910.

(4) All information submitted for clearance to DOPSR must first be coordinated within the originating DoD Component to ensure that it:

(a) Reflects the organization's policy position.

(b) Does not contain classified, controlled unclassified, or critical information requiring withholding.

(c) Is reviewed for operations security in accordance with References (j) and (k).

(d) Is reviewed to ensure there is no risk of releasing classified, controlled unclassified, operations security, or critical information if the information is aggregated with other publicly available data and information in accordance with References (j) and (k).

(5) Only the full and final text of material proposed for release will be submitted for review. Drafts, notes, outlines, briefing charts, etc., may not be submitted as a substitute for a complete text. DOPSR reserves the right to return draft or incomplete documents without action.

(6) Abstracts to be published in advance of a complete paper, manuscript, etc., require clearance. Clearance of an abstract does not fulfill the requirement to submit the full text for clearance before its publication. If an abstract is cleared in advance, that fact, and the DOPSR case number assigned to the abstract, will be noted on the DD Form 1910 or other transmittal when the full text is submitted.

b. Other Requirements. The requirements of References (f) and (l) will apply to the processing of information proposed for submission to Congress.

c. Website Publication. Information intended for placement on websites or other publicly accessible computer servers that are available to anyone requires review and clearance for public release if it meets the requirements of section 1 of this enclosure and DoDI 8550.01 (Reference (p)). Website clearance questions should be directed to the Component's website manager. Review and clearance for public release is not required for information to be placed on DoD controlled websites or computer servers that restrict access to authorized users.

d. Basic Research. Submitters will comply with the DoD guidance on basic scientific and technical research review in DoDI 5230.27 (Reference (q)).

DoDI 5230.29, August 13, 2014

e. Federally Funded Research and Engineering. Submitters will comply with the DoD guidance in federally funded research and engineering in DoDI 3200.12 and DoDI 3200.14 (References (r) and (s)), which requires submitters to send the final published document or final author's referenced manuscript to the Defense Technical Information Center (DTIC).

3. TIMELINES FOR SUBMISSION

a. Prepublication Security and Policy Review Requests

(1) Submit speeches and briefings to DOPSR at least 5 working days before the event at which they are to be presented. Additional time may be needed for complex or potentially controversial speeches due to coordination requirements.

(2) Other material (e.g., papers and articles) will be submitted to DOPSR at least 10 working days before the date needed. The length, complexity, and content will determine the number of agencies required to review the document and, consequently, the time required for the complete review process.

(3) Technical papers will be submitted to DOPSR at least 15 working days before the date needed. More time may be needed if DOPSR determines that the material is complex or requires review by agencies outside of the DoD.

(4) Manuscripts and books will be submitted to DOPSR at least 30 working days before the date needed and before submission to a publisher. More time may be needed if DOPSR determines that the material is complex or requires review by agencies outside of the DoD.

(5) DOPSR reserves the right to return documents without action if insufficient time is allowed for prepublication review.

b. Congressional Security and Policy Review Requests. Security and policy review of material submitted by the DoD to Congress will be provided to DOPSR in these timeframes to allow for a thorough review for DoD to comply with the congressional committee or subcommittee mandates:

(1) Statements: 5 days before submission to the DoD Office of Legislative Counsel in accordance with References (f) and (l).

(2) A minimum of 5 working days for these requests:

(a) Questions for the Record.

(b) Inserts for the Record.

(c) Advance Policy Questions.

DoDI 5230.29, August 13, 2014

- (d) Selected Acquisition Reports.
- (e) Budget documents (in accordance with Reference (f)).
- (f) Classified transcripts only (in accordance with Reference (f)).
- (g) Reprogramming actions.
- (h) Congressional reports.

4. REVIEW DETERMINATIONS AND APPEALS

a. General. Information reviewed for release to the public will result in one of these determinations:

(1) Cleared for Public Release. The information may be released without restriction by the originating DoD Component or its authorized official. DOPSR may require a disclaimer to accompany the information, as follows: “The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.”

(2) Cleared “With Recommendations” for Public Release. Optional corrections, deletions, or additions are included. Although DOPSR has no responsibility for correcting errors of fact or making editorial changes, obvious errors may be identified in the text and noted as “recommended.” These corrections are not binding on the author or submitter.

(3) Cleared “As Amended” for Public Release. Amendments, made in red, are binding on the submitter. Red brackets identify information that must be deleted. If the amendments are not adopted, then the DoD clearance is void. When possible, alternative wording is provided to substitute for the deleted material. Occasionally, wording will be included that must be added to the text before public release. A disclaimer, as shown in paragraph a(1) of this section, may also be required.

(4) Not Cleared for Public Release. The information submitted for review may not be released.

b. Appeals. All amendments or “not cleared” determinations may be appealed in writing by the requester within 60 days to DOPSR. The appeal must contain the basis for release of information denied during the initial determination. All appeals will be resolved at the lowest practical level and as quickly as possible. In accordance with Reference (a), the ~~Director of Administration~~ *DA ODCMO* serves as the appellate authority for any denials or redactions that may be contested. When the appellate authority makes a final determination, a written response will be promptly forwarded to the requester.

DoDI 5230.29, August 13, 2014

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

| | |
|-----------------|---|
| <i>DA ODCMO</i> | <i>Director of Administration, Office of the Deputy Chief Management Officer of the Department of Defense</i> |
| DCMO | Deputy Chief Management Officer <i>of the Department of Defense</i> |
| DoDD | DoD directive |
| DoDI | DoD instruction |
| DOPSR | Defense Office of Prepublication and Security Review |
| WHS | Washington Headquarters Services |

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this instruction.

authorized government representative. A government employee who possesses the authority to communicate a particular component's policies and recommendation for public release.

militarily critical. Information will be considered militarily critical if it addresses any of these subjects or affects the operations security thereof:

New weapons or weapons systems, or significant modifications or improvements to existing weapons or weapons systems, equipment, or techniques.

Military operations and significant exercises of national or international significance.

Command, control, communications, computers, intelligence, surveillance, and reconnaissance; information operations and cyberspace; weapons of mass destruction; improvised explosive devices; and computer security.

Military activities or application in space; nuclear weapons, including nuclear weapons effects research; defense from chemical and biological warfare and threats; initial fixed weapons basing; and arms control treaty implementation.

Any other contemporary topic that is designated by the DoD Component head.

public release. The act of making information available to the public with no restrictions on access to or use of the information. Authorization and release of information to the public, cleared by DOPSR, is the responsibility of the originating office.

EXHIBIT G:

*Frequently Asked Questions for
Department of Defense Security
and Policy Reviews, DOD*
(Mar. 2012)

Frequently Asked Questions for Department of Defense Security and Policy Reviews

What is a security and policy review?

A security and policy review, or pre-publication review, is the process by which information proposed for public release is examined to ensure compliance with DoD and national policies and to determine that it contains no classified, controlled unclassified, or export-controlled information.

Why are these reviews necessary?

The purpose of the security and policy review is to ensure information damaging to the national security is not inadvertently disclosed.

Who must submit materials intended for publication for review by DoD components to Office of Security Review (OSR) for review?

All current, former, and retired DoD employees, contractors, and military service members (whether active or reserve) who have had access to DoD information or facilities. DoD information includes any work that relates to military matters, national security issues, or subjects of significant concern to DoD in general, such as spy novels or biographical accounts of operational deployments and wartime experiences. Publications about gardening, cooking, sports, and crafts and the like do not need to undergo pre-publication

reviews if there is no association with the author's current or former DoD affiliation.

What must go through the security and policy pre-publication review process?

- Books
- Manuscripts and theses
- Biographies
- Articles
- Book reviews/Op-Ed pieces
- Audio/video materials
- Speeches/Presentations
- Press releases/Website updates
- Conference panels/briefings
- Research papers
- Other media

How long will it take?

Specific timelines are addressed in DoDI 5230.29, Enclosure 3, para 3, "Time limits." Note that manuscripts should be submitted for pre-publication review early enough to allow at least 30 working days for the review. Actual review time will vary based on content.

Where do I send my request and what should it include?

First, conduct an Operations Security (OPSEC) review through the Component OPSEC Manager in accordance with DoDM 5205.02.

Then, conduct a pre-publication review. DoDI 5230.29, Enclosure 3, para 2, "Submission Procedures" details what is required. DD Form 1910 is used by active duty personnel and

government officials. A signed letter should be submitted by someone in the private sector and will need to include the following:

- Name
- Contact information (address, phone number, email address)
- Information title or subject
- Intended audience or publication
- Specific deadline, if applicable
- Written consent from all-DoD affiliated personnel named in your material, if applicable.

Include a minimum of three unbound paper copies, or if submitted electronically, one soft copy, of each document in its final form submitted for review.

How does the process work?

The DoD component's security review liaison office (for security/policy review) and their pre-publication release official will:

- Confirm the request qualifies as a pre-publication review and that all required information is included.
- Forward to OSR all requests containing information defined under DoDI 5230.29, Enclosure 3, para 1, in final form.
- Coordinate with other DoD components or offices as necessary prior to submission.

What will happen if I do not submit my material for review?

You may be subject to administrative or legal action.

Reference: USD(I) Memo, "Security and Policy Reviews of Articles, Manuscripts, Books and Other Media Prior to Public Release," April 26, 2011
<https://www.intelink.gov/sites/ousdi/hcis/sec/icedirect/information/default.aspx>

SUBMISSION METHODS

Completed packages should be forwarded to your DoD component organization for initial security review by your public release official.

Personnel assigned to the Office of the Secretary of Defense should forward packages to the Office of Security Review (OSR) – 2A534 - Pentagon or send them to the following address:

Standard mail:

Department of Defense
Attn: Office of Security Review
1155 Defense Pentagon
Washington, DC 20301-1155

Courier:

OSD Mail Room in the Pentagon (3C843)

Email:

NIPR – secrev1@whs.mil (unclassified)
SIPR – ofoisr@whs.smil.mil (FOUO and classified up to SECRET)
JWICS – OfficeofSecurity@osdi.ic.gov (All)

Telephone: (703)-614-5001

Fax: (703)-614-4956

Classified Fax: (703)-614-4966

OSR Website:

www.dtic.mil/whs/esd/osr/index.htm

DoD POLICY FOR SECURITY AND POLICY REVIEWS

Current DoD policy issuances, references and forms governing publication reviews can be found at the OSR Website:
www.dtic.mil/whs/esd/osr/index.htm

These include the following:

DoD Directive 5230.09, "Clearance of DoD Information for Public Release"

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release"
DD Form 1910, "Clearance Request for Public Release of Department of Defense Information"

Related DoD security policy issuances can be found at the DoD issuances website:
<http://www.dtic.mil/whs/directives/>

DoD Manual 5200.01 (Vol. 1 - 4) "DoD Information Security Program"

DoD Manual 5205.02, "DoD Operations Security Program Manual"

For questions on security/policy review submissions or status updates, contact the OSR Help Desk at 703-614-5001.

For questions on information security policy, contact Security Directorate, OUSD(I) at 703-604-2764.

Security and Policy Reviews of Articles, Manuscripts, Books and Other Media Prior to Public Release

Frequently Asked Questions



**Department of Defense
Security Directorate
Office of the Under Secretary of Defense
for Intelligence
5000 Defense Pentagon
Washington, DC
20301-5000**

EXHIBIT H:
NSA/CSS Policy 1-30, *Review
of NSA/CSS Information
Intended for Public Release*
(revised May 12, 2017)

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY 1-30

Issue Date: 13 May 2015
Revised: 12 May 2017



REVIEW OF NSA/CSS INFORMATION INTENDED FOR PUBLIC RELEASE

PURPOSE AND SCOPE

This document sets forth the policy, procedures, and responsibilities governing the prepublication review of official NSA/CSS information intended for public release by current and former NSA/CSS affiliates in either an official capacity or a private capacity. This policy also implements Department of Defense (DoD) Directive 5230.09, "Clearance of DoD Information for Public Release" (Reference a).

This policy applies to all current and former NSA/CSS affiliates and reflects lifetime obligations agreed to in non-disclosure agreements.

/s/

ELIZABETH R. BROOKS
Chief of Staff

/s/

Endorsed by
Associate Director for Policy

Policy 1-30 is approved for public release.

000088

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

DISTRIBUTION:

P12
P13
P131
P134 (Vital Records)

This Policy supersedes NSA/CSS Policy 1-30 dated 10 May 2013. The Chief, Policy approved an administrative update on 12 May 2017 to update organizational designators for NSA21. OPI: Information Security and Classification Division, P131, 972-2534 (secure) or (443)-634-4094 (non-secure).

POLICY

1. Public release in an official capacity:

a. NSA/CSS makes certain accurate and timely information available to the public to promote accountability for and understanding of its activities. The public release of official NSA/CSS information shall be limited only as necessary to safeguard information requiring protection in the interest of national security or other legitimate Government interest ([Reference a](#)). All current NSA/CSS affiliates shall submit for prepublication review all official NSA/CSS information intended for public release in their official capacity. The prepublication review process includes both a classification review and a review that determines whether the information intended for public release: is consistent with established NSA/CSS, DoD, and Intelligence Community policies and programs; is consistent with information security standards established by the Office of Information Management (OIM, P13); and conforms to NSA/CSS corporate messaging standards as determined by Strategic Communications (P2).

b. Official NSA/CSS information prepared as part of official duties and approved for public release will be used in accordance with DoD Directive (DoDD) 5500.07, "Standards of Conduct" ([Reference b](#)), and DoD 5500.7-R, "Joint Ethics Regulation (JER)" ([Reference c](#)), which preclude such use for monetary or nonmonetary personal gain.

2. Public release in a private capacity: NSA/CSS affiliates acting in a private capacity, and not in connection with their official duties, may prepare information for public release without management approval or policy review provided that the affiliate:

- a. Violates no laws or regulations;
- b. Maintains ethical standards and compliance with [References b and c](#);
- c. Uses only information that is UNCLASSIFIED and approved for public release;
- d. Uses no information in which NSA/CSS may have intellectual property rights and must file a new patent application with the U.S. Patent and Trademark Office thereon

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

or lose the right to do so (i.e., the information, if publicly released, does not establish a date by which NSA/CSS must file a new patent application (e.g., 1 year after public release)); and

e. Uses a disclaimer on any material in which an NSA/CSS affiliation is cited, stating that the views and opinions expressed are those of the affiliate and do not reflect those of NSA/CSS.

3. Information available from both classified and open sources:

a. Official NSA/CSS information appearing in the public domain shall not be automatically considered UNCLASSIFIED or approved for public release.

b. Where information intended for public release is available to the NSA/CSS affiliate from classified sources and also independently from open sources, the affiliate may be permitted to release the information if the affiliate can cite an adequate open-source publication where the specific information is available – only if release of the information by the affiliate at the time of review will not cause additional damage to national security through confirmation of previous unauthorized releases. The appropriate Prepublication Review Authority shall exercise discretion in making such determinations on a case-by-case basis and may consider the following as factors in the decision:

- 1) The sensitivity of the information from classified sources;
- 2) The number and currency of the previous releases;
- 3) The level of detail previously exposed;
- 4) The source of the previous releases (whether authoritative and acknowledged or an anonymous leak);
- 5) The submitter's access to classified sources; and
- 6) The authority and credibility afforded by the affiliate's NSA/CSS experience.

4. Official NSA/CSS organizational logos: A logo may be created in accordance with NSA/CSS Policy 10-7, "NSA/CSS Multimedia Information" (Reference d). Once Graphics Services (P2212) creates a proof of the logo, it must be reviewed and approved for public release in an official capacity as set forth in this policy. Once approved for public release, a logo may be used for official NSA/CSS operational, promotional, or morale-building purposes.

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

PROCEDURES

5. For public release in official capacity:

a. Information intended for public release in an NSA/CSS affiliate's official capacity (including, but not limited to, books, articles, videos, speeches, conference briefings, Internet postings, biographies, book reviews, cooperative education (co-op) reports, press releases, research papers, and organizational logos) is subject to prepublication review.

b. Before publicly disclosing his or her NSA/CSS affiliation, a current affiliate preparing material for public release in an official capacity shall seek operations security (OPSEC) guidance from his or her Staff Security Officer (SSO) and solicit a [name check](#) from Chief, NSA/CSS Cover Office (X073) in accordance with NSA/CSS Policy 1-18, "NSA/CSS Cover Program" ([Reference e](#)).

c. Whenever practicable, to preclude the inadvertent spillage of classified information onto unclassified systems, NSA/CSS affiliates acting in an official capacity shall use a TOP SECRET classified information system (e.g., NSANet, JWICS) to draft the full material intended for public release. Notes, outlines, or other partial information may not be substituted for the full material intended for public release in order to avoid the possibility of classification due to compilation.

d. Current NSA/CSS affiliates acting in an official capacity shall first submit, for management review and approval, all official NSA/CSS information intended for public release.

e. Upon receipt of management approval for public release (which may be in the form of a digitally signed email), a current NSA/CSS affiliate acting in an official capacity submits the following to a local [Classification Advisory Officer \(CAO\)](#) for an initial classification determination: the full material intended for public release, management approval, and written consent from NSA/CSS affiliates identified in the information to have any NSA/CSS affiliation publicly revealed. A complete list of CAOs can be found on NSANet ("[go cao](#)").

f. Upon determining the information to be UNCLASSIFIED, the CAO sends a digitally signed email to the affiliate containing that determination.

g. Following procedures established by the Prepublication Review Authority, either the affiliate or the local CAO then forwards the full and final material intended for public release (with all classification markings and/or handling instructions removed), management approval, classification determination, written consent from affiliates identified in the information to have any NSA/CSS affiliation publicly revealed (if applicable), technical review (if applicable), and contracting officer approval (if applicable) to the appropriate NSA/CSS Prepublication Review Authority for the final prepublication review determination.

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

h. The appropriate Prepublication Review Authority shall:

- 1) As necessary, coordinate with other information owners should the material contain information not under his or her purview;
- 2) Refer the information for review to organizations external to NSA/CSS, if required;
- 3) Coordinate, as appropriate, a review with the Public Affairs Office (PAO, P21) to determine that information intended for public release in an affiliate's official capacity conforms to NSA/CSS corporate messaging standards;
- 4) When necessary, request a technical review by a subject matter expert to determine that the information intended for public release is accurate;
- 5) When necessary, request a review by the NSA/CSS Office of the General Counsel (OGC) to determine that the information intended for public release contains no information in which NSA/CSS may have intellectual property rights and may file a patent application thereon; and
- 6) If the current NSA/CSS affiliate acting in an official capacity is a Senior Leader, coordinate with the Information Security and Classification Division (P131) to obtain prepublication approval from the Defense Office of Prepublication and Security Review (DOPSR).

i. The appropriate Prepublication Review Authority will issue, as practicable, a final determination to the affiliate within 25 business days of receipt of all required information and supporting documentation.

6. For public release in a private capacity:

a. Resumes, associated cover letters, work-related biographies (bios), and curriculum vitae (CVs) intended for any public use: Current and former NSA/CSS affiliates shall submit résumés, associated cover letters, work-related bios, and CVs intended for public release to the Information Security and Classification Division (P131) for review according to procedures published on the Information Security and Classification Division (P131) Web site and on nsa.gov to determine whether they contain NSA/CSS protected information.

1) Before publicly disclosing his or her NSA/CSS affiliation in such a document, a current affiliate shall seek OPSEC guidance from an SSO and solicit a name check from Chief, X073.

2) Whenever practicable and with supervisory approval, to preclude the inadvertent spillage of classified information onto unclassified systems, current NSA/CSS affiliates acting in a private capacity may use a TOP SECRET classified information system (e.g., NSANet, JWICS) to draft the full version of such documents intended for public release. Notes, outlines, or other partial

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

information may not be substituted for the full material intended for public release in order to avoid the possibility of classification due to compilation.

3) A current affiliate shall have such documents first reviewed by an organizational CAO before submitting it to P131.

4) Former affiliates shall submit such documents per instructions in [paragraph 6.b.4.](#)

5) Résumés are not subject to management approval or policy review.

b. Other than résumés: Current and former NSA/CSS affiliates may prepare material for public release that meets all of the requirements stated in [paragraph 2.](#) This includes, but is not limited to, books, articles, videos, speeches, conference briefings, Internet postings, book reviews, co-op reports, press releases, research papers, and organizational logos. However, prepublication review is required where compliance with the requirements of [paragraph 2](#) is in doubt (i.e., where the material contains official NSA/CSS information that may or may not be UNCLASSIFIED and approved for public release). Before publicly disclosing an NSA/CSS affiliation, a current affiliate shall seek OPSEC guidance from an SSO and solicit a name check from Chief, X073.

1) Whenever practicable and with supervisory approval, to preclude the inadvertent spillage of classified information onto unclassified systems, current NSA/CSS affiliates acting in a private capacity may use a TOP SECRET classified information system (e.g., NSANet, JWICS) to draft the full material intended for public release. Notes, outlines, or other partial information may not be substituted for the full material intended for public release in order to avoid the possibility of classification due to compilation.

2) A current affiliate with access to a TOP SECRET classified network (e.g., NSANet, JWICS) shall request review by his or her organization's CAO of the full material intended for public release. After review, the organization's CAO will send the full and final material and the initial determination to the appropriate Prepublication Review Authority for a second review.

3) Current affiliates without access to a TOP SECRET classified network (e.g., NSANet, JWICS) may submit the full and final material intended for public release via another classified system (e.g., SIPRNet) to the appropriate Prepublication Review Authority according to established procedures.

4) Former affiliates without access to a TOP SECRET classified network (e.g., NSANet, JWICS) shall submit the full and final material intended for public release in hardcopy to:

NSA/CSS
ATTN: P131, Prepublication Review
9800 Savage Road

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

Suite 6932
Fort George G. Meade, MD 20755-6248

5) The appropriate Prepublication Review Authority shall create an official record of the documents reviewed and the determinations made.

6) As necessary, the appropriate Prepublication Review Authority shall coordinate with other information owners when the material contains information under their purview.

7) The appropriate Prepublication Review Authority shall, as practicable, issue the determination to the affiliate within 25 business days of receipt.

7. Appeal of a prepublication review determination:

a. A prepublication review determination may be appealed in writing to the Chief, OIM within 20 business days of receipt of the determination. At OIM's discretion, an additional 30 business days may be allowed to file a written appeal, provided that the affiliate files a written notice of intent to appeal within 20 business days of receipt of the initial determination and presents justification to support an extension. The affiliate making the appeal shall specifically identify the disputed portions of the initial determination and the reasons for appeal – and shall include any supporting information that the Chief, OIM should consider.

b. In support of OIM, the Information Security and Classification Division (P131) will, if necessary, schedule meetings with the NSA OGC and/or the information owners to review the disputed information and, within 30 business days of receipt of the appeal, advise the affiliate making the appeal of the Chief's OIM final determination and, to the extent consistent with national security, the reasons for any OIM determination adverse to the affiliate's interests.

c. The final determination by the Chief, OIM may not be further appealed.

RESPONSIBILITIES

8. A current NSA/CSS affiliate acting in an official capacity shall:

a. Before disclosing his or her NSA/CSS affiliation, solicit a name check from Chief, X073 in accordance with [Reference e](#);

b. Seek OPSEC guidance from an SSO regarding the possible consequences of disclosing his or her NSA/CSS affiliation;

c. Submit for prepublication review all materials intended for public release according to the procedures specified in [paragraph 5](#);

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

d. As applicable, obtain written consent from each affiliate identified in the information to have his or her NSA/CSS affiliation publicly revealed; and

e. In accordance with established procedures, submit to the appropriate Prepublication Review Authority his or her requests for prepublication review along with all required information identified in [paragraph 5.g.](#).

9. Current NSA/CSS affiliates acting in a private capacity shall:

a. Before disclosing their NSA/CSS affiliation, solicit name checks from Chief, X073 in accordance with [Reference e](#);

b. Seek OPSEC guidance from an SSO regarding the possible consequences of disclosing their NSA/CSS affiliation;

10. Current and former NSA/CSS affiliates acting in a private capacity shall:

a. Submit for prepublication review all materials intended for public release according to the procedures specified in [paragraph 6](#);

b. Notify NSA/CSS of any request to comment on any unofficial NSA/CSS-related information (e.g., to review a book by a non-Government author prior to publication, to review an article). The NSA/CSS affiliate shall regard his/her comments as a proposed unofficial publication subject to review, as provided by this policy. If the appropriate Prepublication Review Authority determines that all or part of the text being commented on must be reviewed in order to evaluate the comments, the affiliate shall obtain permission from the author before submitting relevant parts of any unpublished text to NSA/CSS for review; and

c. As applicable, obtain written consent from each affiliate identified in the information to have his or her NSA/CSS affiliation publicly revealed.

11. Classification Advisory Officers (CAOs) shall:

a. Conduct an initial classification review of information submitted by an affiliate in their supported organizations, in accordance with current NSA/CSS classification and declassification guidance;

b. Provide the affiliate with a digitally signed email message or, if email is not practicable, an appropriately classified letter containing the classification determination; and

c. In accordance with established procedures and on behalf of the affiliate, submit a request for prepublication review to the appropriate Prepublication Review Authority (see [paragraph 5.g.](#)).

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

12. Prepublication Review Authorities shall:

- a. Assist the CAO, when necessary, in resolving classification disputes;
- b. Coordinate reviews, as appropriate, with PAO for conformance to messaging standards;
- c. If the current NSA/CSS affiliate acting in an official capacity is a Senior Leader, coordinate with the Information Security and Classification Division (P131) to obtain prepublication approval from the DOPSR;
- d. Coordinate prepublication reviews with any other NSA/CSS offices as required by, and specified in, this policy;
- e. Coordinate prepublication reviews with external information owners (e.g., U.S. Government, foreign government), as appropriate;
- f. Conduct, as practicable, final prepublication reviews of all information intended for public release within 25 business days of receipt;
- g. Notify the affiliate in writing of the determination; and
- h. Maintain all required electronic and hardcopy official records related to prepublication review determinations in accordance with this policy and NSA/CSS Policy 1-6, "Records Management Program" ([Reference f](#));

13. The Information Security and Classification Division (P131) shall perform all of the functions of a Prepublication Review Authority (see [paragraph 12](#)) and shall:

- a. Serve as the sole approval authority for the public release of personal résumés;
- b. Coordinate with the DOPSR to obtain public release approval when the current NSA/CSS affiliate acting in an official capacity is a Senior Leader;
- c. Review and approve or disapprove management directives and any other procedures developed to implement this policy;
- d. Maintain accountability and a database for all required electronic and hardcopy official records related to prepublication review determinations in accordance with [Reference f](#); and
- e. Administratively assist the Chief, OIM in the processing of prepublication review appeals.

14. The Research Director, in addition to the responsibilities in [paragraph 15](#), shall:

- a. Issue management directives to implement this policy that have been approved by the Information Security and Classification Division (P131);

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

b. Provide a monthly accounting of prepublication review cases to the Information Security and Classification Division (P131); and

c. Grant the Information Security and Classification Division (P131) access to any databases used for the electronic storage and tracking of prepublication review cases.

15. The Directors, Cryptologic Center Commanders/Chiefs, and Field Commanders/Chiefs shall:

a. Develop a process, consistent with the provisions in this policy, for ensuring the proper prepublication review of official NSA/CSS information intended for public release;

b. Ensure that personnel under their supervision are made aware of the requirements of this policy; and

c. Ensure that subordinates' requests for management review and approval of official NSA/CSS information intended for public release pursuant to [paragraph 5.b](#) are completed in a timely manner.

16. The Security and Counterintelligence Group (A5) shall:

a. Ensure that, during initial indoctrination, all affiliates are informed of their lifelong responsibility to safeguard NSA/CSS protected information and of the procedures for prepublication review;

b. Ensure that all affiliates are reminded of their lifetime prepublication review responsibilities prior to signing their security debriefing forms at the end of their affiliation with the Agency; and

c. Via SSOs, provide OPSEC guidance to current affiliates regarding the possible consequences of publicly disclosing their NSA/CSS affiliation when preparing official NSA/CSS information for public release in either an official or private capacity.

17. The Office of General Counsel (OGC) shall:

a. Provide legal advice to a Prepublication Review Authority when material intended for public release contains any information in which NSA/CSS may have intellectual property rights and may file a patent application thereon;

b. Ensure, in coordination with the Business Management and Acquisition Directorate (B), that contracts contain necessary provisions to require compliance with the provisions of this policy by contractors and their employees; and

c. Provide legal advice and guidance to the Information Security and Classification Division (P131) and Chief, OIM during the appeal process, as necessary and as required.

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

18. The Business Management and Acquisition Directorate (BM&A) shall ensure, in coordination with the OGC, that contracts contain necessary provisions to require compliance with the provisions of this policy by contractors and their employees.

19. The Public Affairs Office (PAO) shall, as appropriate, perform a review on all information intended for public release in an official capacity within 10 business days of receipt to ensure that information intended for public release conforms to current NSA/CSS messaging standards as determined by Strategic Communications.

20. The Chief, NSA/CSS Cover Office (X073) shall conduct name checks as requested by current affiliates preparing official NSA/CSS information for public release in either an official or private capacity in accordance with [Reference e.](#)

REFERENCES

21. References:

- a. [DoDD 5230.09](#) "Clearance of DoD Information for Public Release," dated 22 August 2008.
- b. [DoDD 5500.07](#), "Standards of Conduct," dated 29 November 2007.
- c. [DoD 5500.7-R](#), "Joint Ethics Regulation (JER)," dated 1 August 1993.
- d. [NSA/CSS Policy 10-7](#), "NSA/CSS Multimedia Information," dated 12 August 2009 and revised 1 May 2013.
- e. [NSA/CSS Policy 1-18](#), "NSA/CSS Cover Program," dated 6 March 2014.
- f. [NSA/CSS Policy 1-6](#), "Records Management Program," dated 19 November 2014.
- g. [Executive Order 13526](#), "Classified National Security Information," dated 25 January 2010.
- h. [Public Law No. 86-36](#) (codified as amended in 50 U.S.C. § 3605), "National Security Agency Act of 1959."
- i. [5 U.S.C § 552](#), "Freedom of Information Act."

DEFINITIONS

22. [Affiliate](#) – A person employed by, detailed to, or assigned to NSA/CSS, including a member of the U.S. Armed Forces; an expert or consultant to NSA; an industrial or commercial contractor, licensee, certificate holder, or grantee of NSA, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of NSA/CSS as determined by the Director, NSA/Chief, CSS. (Source: [NSA/CSS Policy Glossary](#))

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

23. Classification Advisory Officer (CAO) – An individual trained to properly apply classification rules and guidance and who assists other employees in the proper marking and protection of classified and protected information. The Information Policy and Classification Division (P131) administers the CAO Program and registers CAOs. For more information “go CAO.”

24. Logo – An unclassified graphical representation of an NSA/CSS-related special office, mission, program, or project.

25. Name Check – A review of past assignments, including assignments to other agencies and participation in educational programs, to determine the classification of an individual’s name in association with NSA/CSS ([Reference e](#)).

26. Nondisclosure Agreement (NdA) – A lifetime obligation to safeguard all protected information, to submit all information intended for publication and/or public release for prepublication review, and to report any unauthorized disclosure of protected information. NSA/CSS affiliates are legally bound and obligated by any NdAs they sign for access to NSA/CSS information. They shall not confirm or deny information about NSA/CSS that appears in the public domain without prior approval through the classification or prepublication process.

27. NSA/CSS Protected Information – Information obtained as a result of a relationship with NSA/CSS, that is:

a. Classified or in the process of a classification determination pursuant to the standards of Executive Order 13526 ([Reference g](#)), or any successor order, and implementing regulations. It includes, but is not limited to, intelligence information, sensitive compartmented information (intelligence sources and methods), and cryptologic information (information concerning information systems security and signals intelligence); or

b. Unclassified, appearing in any form or compilation, which NSA/CSS may withhold from public disclosure under authority of the National Security Agency Act of 1959 ([Reference h](#)) or by reason of being either excluded or exempted from the mandatory disclosure requirements of the Freedom of Information Act ([Reference i](#)). (Source: [NSA/CSS Policy Glossary](#))

28. Official Capacity – Acting on behalf of NSA/CSS.

29. Official NSA/CSS Information – Any NSA/CSS, DoD, or IC information that is in the custody and control of NSA/CSS and was obtained for or generated on NSA/CSS’ behalf during the course of employment or other service, whether contractual or not, with NSA/CSS.

30. Prepublication Review – The overall process to determine that information proposed for public release contains no protected information and, where applicable, is consistent with established NSA/CSS, DoD, and IC policies and programs; conforms to NSA/CSS messaging standards as determined by Strategic Communications; and, in consultation with the NSA OGC,

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

Policy 1-30

Dated: 13 May 2015

Acquisition, Research, and Technology Law Practice, as appropriate, contains no information in which NSA/CSS may have intellectual property rights and may file a patent application thereon.

31. Prepublication Review Authority – Officials in organizations who are delegated the authority to make determinations on prepublication reviews. The Information Security and Classification Division (P131) serves as the corporate-level Prepublication Review Authority and as such has the authority to make a determination on any prepublication review and has sole authority for the prepublication review of personal résumés, associated cover letters, bios, and CVs. The Chief, Office of Information Management (OIM, P13) has officially delegated Prepublication Review Authority to the Research Directorate for review of RD-related, non-résumé material and/or non-résumé material submitted by RD personnel.

32. Private Capacity – Acting on behalf of oneself and not in association with NSA/CSS.

33. Public Release – The decision to give permission to retain, or to show or reveal official NSA/CSS information whether orally, in writing, or through any other medium, to one or more persons who otherwise do not have the appropriate access authorization, security clearance, and/or need to know to receive such information upon determination that the release will not harm the national security or another legitimate Government interest.

34. Senior Leader – A Defense Intelligence Senior Executive Service (DISES) employee, a Defense Intelligence Senior Level (DISL) employee, or the military equivalent of a DISES or DISL employee.

35. Unauthorized Disclosure – Absent a public release, the communication or physical transfer of protected information to one or more unauthorized recipients who do not have appropriate access authorization, security clearance, and/or need to know to receive such information.

EXHIBIT I:

Form 313, *Nondisclosure
Agreement for Classified
Information*
(Dec. 2016)

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

NONDISCLOSURE AGREEMENT FOR CLASSIFIED INFORMATION

1. I, _____ (print full name), hereby agree to accept the obligations contained in this agreement as a prior condition of my being given access to information or material by the United States Government (U.S. Government) that is classified, or is in the process of a classification determination, in accordance with the standards set forth in Executive Order 13526 as amended or superseded, or other applicable Executive order.

2. I understand that such information if disclosed in an unauthorized manner would jeopardize intelligence activities of the U.S. Government. I accept that by being granted access to such information or material I will be placed in a position of special confidence and trust and become obligated to protect that information and/or material from unauthorized disclosure.

3. In consideration for being provided access to information or material by the U.S. Government that is classified, or is in the process of a classification determination in accordance with the standards set forth in Executive Order 13526 as amended or superseded, or other applicable Executive order, I hereby agree that I will never disclose in any form or any manner, to any person not authorized by the U.S. Government to receive it, any information or material in either of the following categories:

a. information or material, including oral communications, received or obtained pursuant to this agreement with the U.S. Government that is marked as classified or that I have been informed or otherwise know is classified;

b. information or material, including oral communications, received or obtained pursuant to this agreement with the U.S. Government that I have been informed or otherwise know is in the process of a classification determination.

4. I understand that it is my responsibility to consult with appropriate management authorities in the U.S. Government component that has sponsored my access, or with the prepublication review component of the agency that gave or sponsored my access to classified information if I am no longer associated with the U.S. Government, in order to know: 1) whether information or material within my knowledge or control that I have reason to believe might be in either of the categories set forth in paragraph 3 is considered by the U.S. Government to fit in either of those categories; and, 2) whom the U.S. Government has authorized to receive such information or material.

5. As a further condition of the special confidence and trust reposed in me by the U.S. Government, I hereby agree to submit for review by the U.S. Government, any writing or other preparation in any form, including a work of fiction, which contains any mention of intelligence data or activities, or which contains any other information or material that might be based upon either of the categories set forth in paragraph 3, that I contemplate disclosing publicly or that I have

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

actually prepared for public disclosure, either during my service with the U.S. Government or at any time thereafter, prior to discussing it with or showing it to anyone who is not authorized to have access to the categories set forth in paragraph 3. I further agree that I will not take any steps toward public disclosure until I have received written permission to do so from the U.S. Government.

6. I understand that the purpose of the review described in paragraph 5 above is to give the U.S. Government an opportunity to determine whether the information or material that I contemplate disclosing publicly contains any information or material that I have agreed not to disclose in accordance with paragraph 3. I further understand that the U.S. Government will act upon my submission and make a response to me within a reasonable time. I further understand that if I dispute the U.S. Government's initial determination on the basis that the information in question derives from public sources, I may be called upon to specifically identify such sources. My failure or refusal to do so may itself result in denial of permission to publish or otherwise disclose the information or material in dispute. I further understand that when otherwise classified information is also available independently in open sources and can be cited by the author the U.S. Government will consider that fact in making its determination on whether the information may be published with the appropriate citations, but I recognize that the U.S. Government retains the right to disallow certain open-source information or citations where, because of the author's U.S. Government affiliation and position the reference might confirm the classified content.

7. I understand that all information or material that I may acquire pursuant to this agreement with the U.S. Government that fits either of the categories set forth in paragraph 3 of this agreement are and will remain the property of the U.S. Government unless or until otherwise determined by an authorized Executive branch official or final ruling of a court of law. I agree that I will not use such information or material for any personal or non-official purposes. I also agree to surrender anything constituting, containing or reflecting such information or material upon the conclusion of my employment or other service with the U.S. Government. I further agree to surrender anything constituting, containing, or reflecting such information or material, upon demand by an appropriate official of the U.S. Government.

8. I agree to notify the U.S. Government immediately in the event that I am called upon by judicial or Congressional authorities, or by specially established investigatory bodies of the Executive branch, to testify about, or provide, information or material that I have agreed herein not to disclose. In any legally authorized communications with any such authority or body, I shall observe all applicable rules or procedures for ensuring that information and/or material that is classified or in the process of a classification determination is handled in a secure manner.

9. I understand that nothing contained in this agreement prohibits me from reporting intelligence activities that I consider to be unlawful or improper directly to the Intelligence Oversight Board established by the President, or to any successor body that the President may establish, or to the Senate Select Committee on Intelligence or the House Permanent Select Committee on Intelligence. I recognize that there are also established procedures for bringing such matters to the attention of Inspector General of the agency that gave or sponsored my access to classified information or to the head of the agency that gave or sponsored my access to classified

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

information. In making any report referred to in this paragraph, I will observe all applicable rules and procedures for ensuring the secure handling of any information or material that may be involved. I understand that any such information or material continues to be subject to this agreement for all other purposes and that such reporting does not constitute public disclosure or declassification of that information or material.

10. I understand that any breach of this agreement by me may result in the U.S. Government taking administrative action against me, if applicable, which can include suspension or termination of my security clearance and relationship with the U.S. Government. I understand that if I violate the terms of this agreement, the U.S. Government may institute a civil proceeding to seek damages or other appropriate relief. Further, I understand that the disclosure of information that I have agreed herein not to disclose can, in some circumstances, constitute a Federal criminal offense.

11. I understand that the U.S. Government may, prior to any unauthorized disclosure that is threatened by me, choose to apply to any appropriate court for an order enforcing this agreement. Nothing in this agreement constitutes a waiver on the part of the United States to institute a civil or criminal proceeding for any breach of this agreement by me. Nothing in this agreement constitutes a waiver on my part of any possible defenses I may have in connection with either civil or criminal proceedings that may be brought against me.

12. In addition to any other remedy to which the U.S. Government may become entitled, I hereby assign to the U.S. Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any divulgence, publication, or revelation of information or material by me that is carried out in breach of paragraph 5 of this agreement or that involves information or material prohibited from disclosure by the terms of this agreement.

13. I understand and accept that, unless I am provided a written release from this agreement or any portion of it by the head of the agency that gave or sponsored my access to classified information or his or her authorized representative, all the conditions and obligations accepted by me in this agreement apply during my service with the U.S. Government, and at all times thereafter.

14. I understand that the purpose of this agreement is to implement the protection of intelligence sources and methods under the National Security Act of 1947, as amended, and Executive Order 12333, as amended.

15. Nothing in this agreement bars disclosures to Congress or disclosures to an authorized official of an executive agency that are deemed essential to reporting of a violation of United States law.

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

16. I understand that nothing in this agreement limits or otherwise affects any provision of criminal or other law that may be applicable to the unauthorized disclosure of classified information, including the espionage laws (sections 793, 794 and 798 of title 18, United States Code) and the Intelligence Identities Act of 1982 (P.L. 97-200; 50 U.S.C. §3121 *et. seq.*).

17. Each of the numbered paragraphs and lettered subparagraphs of this agreement is severable. If a court should find any paragraphs or subparagraphs of this agreement to be unenforceable, I understand that all remaining provisions will continue in full force.

18. I make this agreement in good faith, and with no purpose of evasion.

19. This agreement shall be interpreted under and in conformance with the law of the United States.

Signature

Date

Social Security Number (See Notice below)

The execution of this agreement was witnessed by the undersigned, who accepted it on behalf of the U.S. Government as a prior condition of access to classified information by the person whose signature appears above.

WITNESS AND ACCEPTANCE:

Signature

Printed Name

Date

Page 4 of 5

FORM 313
(Rev. 12-16)

000004

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

EXHIBIT J:

Instruction 80.04, Revision 2,
*ODNI Pre-Publication Review
of Information to Be Publicly
Released*

(effective Aug. 9, 2016)

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
INSTRUCTION 80.04**

Category 80 - Information and Records Management
Office of Primary Responsibility: Assistant Director of National
Intelligence for Policy and Strategy/
Information Management Division
Revision 2

**SUBJECT: ODNI PRE-PUBLICATION REVIEW OF INFORMATION TO BE
PUBLICLY RELEASED**

1. AUTHORITIES: The National Security Act of 1947, as amended; and other applicable provisions of law.

2. REFERENCES: Executive Order (E.O.) 12333, as amended; E.O. 13526; *Intelligence Community Markings System Register and Manual*; and the *Office of the Director of National Intelligence (ODNI) Classification Guide*.

3. PURPOSE: This Instruction establishes the requirements and responsibilities in the ODNI for pre-publication review of all information that is to be released publicly. The goal of pre-publication review is to prevent the unauthorized disclosure of information, and to ensure the ODNI's mission and the foreign relations or security of the U.S. are not adversely affected by publication. This Instruction replaces ODNI Instruction 80.04, *ODNI Pre-publication Review of Information to be Publicly Released*, dated April 8, 2014.

4. APPLICABILITY: This Instruction applies to current and former ODNI permanent cadre employees; ODNI staff reserve (i.e., time-limited) cadre employees, including Highly Qualified Experts; federal civilian detailees; military detailees; Intergovernmental Personnel Act detailees; Presidential appointees; assignees; and contractors. In accordance with any relevant agreement by the ODNI and other government agencies (OGAs), this Instruction also applies to OGA employees providing service support to the ODNI. The above listed group will be referred to collectively as "individuals" in this Instruction.

UNCLASSIFIED
000111

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
UNCLASSIFIED

5. DEFINITIONS:

A. **Chatham House Rule:** An understanding, spoken or unspoken, that during academic discussions, the topics discussed and opinions relayed will NOT be attributed to individuals or organizations. This rule is intended to allow the free discussion of academic ideas and opinions without attribution.

B. **Non-official publication:** The category of publications created by individuals for personal, professional, or commercial use that will be made available to the public (e.g., resumes, books, op-eds, personal blogs, performance evaluation reports [PERs] for personal use).

C. **Official publication:** The category of publications created by individuals as part of their duties on behalf of the ODNI, the DNI, the Intelligence Community (IC), or the U.S. Government (USG) that will be made available to the public (e.g., speeches, newsletters, official web pages, outreach documents, brochures).

D. **Publication:** Any information created in part (co-authored) or wholly by individuals intended for release outside the control of the USG, regardless of the medium by which it will be released (i.e., written, voice, or electronic) that discusses any information related to the ODNI, the IC, or national security.

E. **Release:** Allowing information to be made available to the public.

6. **POLICY:** The ODNI has a security obligation and legal responsibility under E.O. 12333 and E.O. 13526 to safeguard sensitive intelligence information and prevent its unauthorized publication as defined in paragraph 5.D. The Director, Information Management Division (D/IMD), serves as the ODNI authority for approval of all ODNI public release reviews. All individuals are required to submit all official and non-official information intended for publication that discusses the ODNI, the IC, or national security. Any 'For Official Use Only' (FOUO) information intended for State, Local, Tribal, and Public Sector (SLTP) must be approved by the IMD. The IMD will coordinate, as necessary, with the Assistant DNI for Partner Engagement (ADNI/PE) on any FOUO information to be shared with foreign partners. FOUO information disseminated within the USG (e.g., Departments of State, Defense, Homeland Security, Treasury) does not require an IMD review. Pre-publication review must be conducted before any uncleared individuals can receive the information, and before the material is sent for peer review via unclassified channels. This Instruction does not release individuals from their obligation to fully comply with nondisclosure agreements (NDAs), nor does it authorize individuals to alter the terms of such agreements. In case of any conflict between this Instruction and an NDA, the NDA shall govern. ODNI pre-publication reviews will be executed as follows:

A. **Pre-submission:** Individuals must initiate a request for approval for the publication of information and conform to the following guidance:

(1) **Classification:** The individual initiating the request must ensure all draft documents

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
UNCLASSIFIED

are correctly classified and portion marked prior to submission for review. See the *IC Markings System Register and Manual* and the current *ODNI Classification Guide* for guidance on correct classification and markings.

(2) Sourcing: Correct unclassified sourcing is critical in executing pre-publication review. Individuals must not use sourcing that comes from known leaks, or unauthorized disclosures of sensitive information. The use of such information in a publication can confirm the validity of an unauthorized disclosure and cause further harm to national security. Individuals are not authorized to use anonymous sourcing.

(3) The Public Affairs Office (PAO) will ensure that official information intended for public release is consistent with the official ODNI position or message. The PAO will approve or disapprove the use of official ODNI seals and letterhead associated with the intended release, as deemed appropriate.

(4) Individuals must obtain supervisor approval for official publication requests, in accordance with internal review requirements of their component, before submitting information for pre-publication review.

(5) Contractual deliverables that will be publicly released must receive approval of the Contracting Officer (CO) or the Contracting Officer's Technical Representative (COTR) prior to submission for pre-publication review. The written approval from the CO or COTR must be included in the submission for review.

(6) Individuals must, prior to participating in open discussion venues such as forums, panels, round tables, and questions and answer (Q&A) sessions, either in-person or online, comply with the following conditions:

(a) Individuals must obtain approval from the PAO to represent the ODNI in any capacity at any public forum.

(b) Individuals expecting to engage in unstructured or free-form discussions about operations, business practices, or information related to the ODNI, the IC, or national security must prepare an outline of the topics to be discussed or the agenda to be followed, and provide to the IMD anticipated potential questions and ODNI responses.

(7) Disclaimer: Approval of non-official publications does not imply endorsement by the ODNI, IC, or national security. Any opinions offered by individuals must be clearly marked as official ODNI or USG positions, or contain a disclaimer that the opinions are not those of the ODNI or USG. The following disclaimer is an example for a non-official publication created by an individual who expresses an opinion about the ODNI, IC, or USG:

"The views expressed in (this publication/these remarks) are the author's and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. Government agency."

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
UNCLASSIFIED

Disclaimers are not required for PERs, resumes, bios, or as others exempted by the D/IMD.

B. Submission: Individuals must submit requests electronically via email to DNI-Pre-Pub. Requests must include results from all previous pre-publication requests for the same information. Publication requests made through the Outside Activities Report (OAR) database must also include a separate email submission to DNI-Pre-Pub@cia.ic.gov (classified) or DNI-Pre-Pub@dni.gov (unclassified) for final approval. Exceptions are as follows:

(1) Former individuals assigned to the ODNI who, lacking access to classified email, will submit requests to DNI-Pre-Pub@dni.gov and ensure their publications have been clearly sourced to unclassified information prior to transmittal.

(2) Detailees and assignees will submit requests for non-official publications to their home agency, provided the home agency has an established publication review process. The IMD will assist those detailees and assignees uncertain of how to submit requests to their home agency.

(3) The Director, Intelligence Advanced Research Projects Agency (D/IARPA), or designee, is delegated the authority to review and publicly disseminate official IARPA technical publications independent of the review process outlined in this Instruction.

C. Review:

(1) The IMD will lead the coordination with all USG agencies and internal ODNI subject matter experts (SMEs) that have equities in a submitted request. The IMD will de-conflict any issues on responses from separate agencies and from within the ODNI, and will provide a single and final response to the requester.

(2) Timelines for review are determined by type of request, complexity of subject, SME time constraints, and requester deadlines. General time lines for reviews are:

(a) For Official Publications: The IMD will complete a review of official publication requests no later than 15 business days from the receipt of the request, as priorities and resources allow.

(b) For Non-Official Publications: The IMD will complete a review of non-official publication requests no later than 30 calendar days from the receipt of the request, as priorities and resources allow.

(3) Requesters must not assume approval in cases where the IMD's reply has not been received by the time guidelines described in this Instruction. It is the responsibility of the requester to protect the information until a formal approval is provided.

D. Re-submission: In the event that a request for public release is denied in whole or in part by the IMD, the requester may resubmit the request to the IMD for a second review. The

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
UNCLASSIFIED

resubmittal must include results from the initial pre-publication requests, and must include additional information and/or a revised draft.

E. Appeal: If publication is denied by the IMD for a second time, the requester may submit a written appeal to the IMD no later than 30 calendar days from the date of the denial. The IMD will coordinate the appeal process. Appeal documentation must include the information intended for publication and any supporting materials to be considered. The IMD will provide the information to the Chief Management Officer (CMO) for final decision. The CMO will receive support from any USG agency and internal ODNI SMEs in the appeal decision, as appropriate. The CMO will issue a final decision, through the IMD, to the requester as time and resources allow.

F. Consequences for non-compliance: Failure to comply with this Instruction may result in the imposition of civil and administrative penalties, and may result in the loss of security clearances and accesses.

G. Non-attribution during discussions (Chatham House Rule): Individuals who participate in environments where the Chatham House Rule applies are not authorized to discuss information or topics that are not authorized for public release. Information that is deemed sensitive or classified due to attribution to the IC or USG cannot be discussed under the Chatham House Rule.

7. RESPONSIBILITIES:

A. The Chief Management Officer will:

- (1) Provide oversight for this policy and the pre-publication review process.
- (2) Issue final decisions on all formal appeals from requesters.

B. The Director, Information Management Division, or designee, will:

- (1) Implement this Instruction.
- (2) Serve as the approval authority for public release of ODNI information to the public, based on classification, policy, and other applicable authorities.
- (3) Coordinate timely pre-publication reviews with all appropriate ODNI components and USG agencies. This includes obtaining, as necessary, additional information from the requester, clarification of purpose, and to make a final determination.
- (4) Provide all staff support to the CMO in the appellate process, to include the preparation of all necessary appeal information to be presented to the CMO.

Approved for Release on 18-Sep-2018, FOIA Case #DF-2018-00189
UNCLASSIFIED

(5) Maintain records for all pre-publication review requests, dispositions, and associated actions.

C. The Director, Public Affairs Office, or designee, will:

(1) Determine if individuals are authorized to officially represent the ODNI, the IC, or USG publicly.

(2) Review official publications for accuracy, clarity, and consistency of ODNI message as part of the pre-publication review process.

D. The Director, Intelligence Advanced Research Projects Agency, or designee, will exercise authority granted in this Instruction to review and publicly disseminate any official IARPA technical publications independent of the review process outlined in this Instruction.

E. Component Directors will, when requested by the D/IMD, designate one or more component SMEs as appropriate, either permanently or on a case-by case basis, to participate in pre-publication reviews. SMEs will limit the scope of their reviews to their component's area of expertise, and provide comments solely on the appropriateness of the information under review for public release.

8. EFFECTIVE DATE: This Instruction is effective upon signature.


Mark W. Ewing
Chief Management Officer

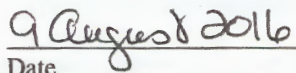

Date

EXHIBIT K:

Standard Form 312, *Classified
Information Nondisclosure
Agreement*
(revised July 2013)

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 13526, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of sections 641, 793, 794, 798, *952 and 1924, title 18, United States Code; *the provisions of section 783(b), title 50, United States Code; and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of sections 793 and/or 1924, title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

(Continue on reverse.)

11. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 13526 (75 Fed. Reg. 707), or any successor thereto section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b) (8) of title 5, United States Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an inspector general, the inspectors general of the Intelligence Community, and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h(g)(3)) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403g(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, *952 and 1924 of title 18, United States Code, and *section 4 (b) of the Subversive Activities Control Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

12. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Part 2001, section 2001.80(d)(2)) so that I may read them at this time, if I so choose.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

| | | |
|-----------|------|--|
| SIGNATURE | DATE | SOCIAL SECURITY NUMBER <i>(See Notice below)</i> |
|-----------|------|--|

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or print)*

| WITNESS | | ACCEPTANCE | |
|--|------|---|------|
| THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED. | | THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT. | |
| SIGNATURE | DATE | SIGNATURE | DATE |
| NAME AND ADDRESS <i>(Type or print)</i> | | NAME AND ADDRESS <i>(Type or print)</i> | |

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

| | |
|-----------------------|------|
| SIGNATURE OF EMPLOYEE | DATE |
|-----------------------|------|

| | |
|--|----------------------|
| NAME OF WITNESS <i>(Type or print)</i> | SIGNATURE OF WITNESS |
|--|----------------------|

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Public Law 104-134 (April 26, 1996). Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above or to determine that your access to the information indicated has been terminated. Furnishing your Social Security Number, as well as other data, is voluntary, but failure to do so may delay or prevent you being granted access to classified information.

EXHIBIT L:

Form 4414, *Sensitive
Compartmented Information
Nondisclosure Agreement*
(revised Dec. 2013)

Apply appropriate classification level and any control markings (if applicable) when filled in.

(U) SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement between

(Name – Printed or Typed)

and the United States.

1. (U) Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or is in process of a classification determination under the standards of Executive Order 13526 or other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.

2. (U) I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. (U) I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be, or related to or derived from SCI, is considered by such Department or Agency to be SCI. I further understand that I am also obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.

4. (U) In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation with, or show it to, anyone who is not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.

5. (U) I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 sets forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon it, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.

6. (U) I have been advised that any breach of this Agreement may result in my termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. (U) I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorney's fees incurred by the United States Government may be assessed against me if I lose such action.

8. (U) I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code.

9. (U) Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all conditions and obligations imposed on me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.

10. (U) Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other

Apply appropriate classification level and any control markings (if applicable) when filled in.

conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

11. (U) I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798 and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 13526, as amended, so that I may read them at this time, if I so choose.

12. (U) I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

13. (U) These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

14. (U) These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations rights or liabilities created by Executive Order 13526; or any successor thereto, Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosures to Congress by members of the Military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosure of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an inspector general, the inspectors general of the Intelligence Community; and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h(g)(3)) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the CIA Act of 1949 (50 U.S.C. 403q(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect agent disclosure which may compromise the national security, including Section 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Control Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

15. (U) This Agreement shall be interpreted under and in conformance with the law of the United States.

16. (U) I make this Agreement without any mental reservation or purpose of evasion.

Signature

Date

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

WITNESS and ACCEPTANCE:

Signature

Date

SECURITY BRIEFING / DEBRIEFING ACKNOWLEDGMENT

(Special Access Programs by Initials Only)

SSN (See Notice Below)

Printed or Typed Name

Organization

BRIEF

Date _____

I hereby acknowledge that I was briefed on the above SCI Special Access Program(s):

Signature of Individual Briefed

DEBRIEF

Date _____

Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on the above SCI Special Access Program(s):

Signature of Individual Briefed

I certify that the briefing presented by me on the above date was in accordance with relevant SCI procedures.

Signature of Briefing/Debriefing Officer

SSN (See notice below)

Printed or Typed Name

Organization (Name and Address)

(U) NOTICE: The Privacy Act, 5 U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397, as amended. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations.